Walkthrough

Step 0: Tooling that may be useful:

- **https://www.base64decode.org/**
- Login teacher on 172.16.1.27:
    - username: root
    - password: root

Step 1: Share credentials with students
You share the following IP-address and login credentials for the students:

- Openvpn file
    - If using your own machine:
        - apt install openvpn
        - apt install openconnect
        - openconnect vpnseclab.fhict.nl
            - Login with your seclab credentials (i-account)
        - wget https://pastebin.com/raw/jtKaqn3U
        - mv jtKaqn3U rvb.ovpn
        - openvpn rvb.ovpn
            - User: vpnuser
            - Password: vpn
- CTF portal (for students) - 172.16.1.27
    - Username: user1
    - Password: user1
- Wazuh (SIEM environment) - 172.16.1.13
    - Username: wazuh
    - Password: xBTM0xG4tCvC-SrkFC2Yert016VHr7dQ
- TheHive
    - Username: user@rvb.nl
    - Password: 88%M!cjOqJ5%cx
- Vulnerable machines:
    - Username: admin
    - Password: password

Step 2: Start game
A teacher can start the game when all of the students are ready to go.

Step 3: Reset game
When the game is finished the teacher can reset the game on the teacher portal.

Extra step: Flag storyline help
This step shows what needs to be done for each step. This is only for information when student(s) do not find their way and need some assistants.

The following steps need to be done in order from 1 to 6:

1: Info systemen

Flag 1: SQL Injection flag = { } (HIGHLIGHT TO REVEAL)
Sub flags: 4

Sub flag: 1/4
Solution: On the Wazuh dashboard, under Security Events, an alert appears:
- *"Suricata: Alert - Possible SQL Injection Attack"*

Flag partial: RDMk
Important URL: http://172.16.1.26:9000/index.html#!/login

Sub flag: 2/4
Solution: In Hive(SIEM), there's a case called SQL Information Leak - open the case and read the description
- *"Case # 3 - SQL Information Leak"*

Flag partial: Tx4i
Important URL: http://172.16.1.26:9000/index.html#!/case/~~78016/details

Sub flag: 3/4
Solution: In Hive(SIEM), open the tasks attached to the previous case and expand
- *"Execute command found in data.http.url"*

Flag partial: jxHZ
Important URL: http://172.16.1.26:9000/index.html#!/case/~~78016/tasks/~~45240

Sub flag: 4/4
Solution: Open the page that was found in the alert; executing the command used is optional
- *"Information system - SQL Injection"*

Flag partial: 0h8}
Important URL: http://172.16.1.15:5001/vulnerabilities/sqli/

Flag: { } (HIGHLIGHT TO REVEAL)

2: Train entrance system

Flag 2: XSS flag = { } (HIGHLIGHT TO REVEAL)
Sub flags: 5

Description: On the Wazuh dashboard, under Security Events, an alert appears:
Suricata: High Alert - XSS attack detected on Train entrance system(s)
Flag partial: 0pr

http://172.16.1.26:9000/index.html#!/login

Description: In Hive(SIEM), there's a case called XSS attack detection - open the case and read the description
Case # 4 - XSS Attack IR
Flag partial: bW5

http://172.16.1.26:9000/index.html#!/

Description: In Hive(SIEM), open the tasks attached to the previous case and expand
Visit the page in which an XSS attack was detected and review if its contents has been defaced;
Flag partial: Whf

http://172.16.1.26:9000/index.html#!/

Description: Open the URL that raised the XSS alert
If the page has been defaced contact the customer using the template below
Flag partial: p9w

Description: In Hive(SIEM), open the last task described as customer contact, in the template there's the last flag
Flag partial: TOx

Flag: {0prbW5Whfp9wTOx}

3: Communication System Attack
Flag 3: CSRF flag = {Er4XCumRFhVEC0t}

Description: On the Wazuh dashboard, under Security Events, an alert appears:
Suricata: Alert - CRITICAL: Detected CSRF on Train entrance systems
Flag partial: Er4

http://172.16.1.26:9000/index.html#!/login

Description: In Hive(SIEM), there's a case called CSRF detection - open the case and read the description
Case # 4 - CSRF Attack IR
Flag partial: XCu

Description: In Hive(SIEM), open the tasks attached to the previous case and expand
Do NOT open the url found in the alert!
Flag partial: mRF

Description: In Hive(SIEM), open the task about incident response;
Either curl the page to see its contents and reset the admin password
Flag partial: hVE

Description: In Hive(SIEM), open the last task described as customer contact, in the template there's the last flag
Flag partial: C0t

Flag: {Er4XCumRFhVEC0t}

4: Railway crossing Attack
Flag 4: Weak Session Id flag = {Fm1AyI1Y9QSH9yP}

Description: On the Wazuh dashboard, under Security Events, an alert appears:
Suricata: Alert - CRITICAL: Unauthorized Access Railway Crossing systems
Flag partial: Fm1A

http://172.16.1.15:5004/vulnerabilities/weak_id/

Description: On the docker dvwa on port 5400 the second partial can be found.
Flag partial: yI1Y9

http://172.16.1.26:9000/index.html#!/login

Description: In Hive(SIEM), open the tasks attached to the previous case. Here can te flag be found..
Flag partial: QSH9yP

5: Speedup/jam attack
Flag 5: Javascript flag = {U25cs71YWJrFagL}

Description: On the Wazuh dashboard, under Security Events, an alert appears:
Suricata: Alert - VERY CRITICAL: Malicious code injection detected on Train system #5344
Flag partial: U25

http://172.16.1.26:9000/index.html#!/login

Description: In Hive(SIEM), there's a case called Malicious Code Injection detection
Case # 7 - Malicious Code Injection into Trainsystems
Flag partial: cs7

Description: In Hive(SIEM), open the tasks attached to the previous case and expand Open the page and review if any malicious code has been injected
Flag partial: 1YW

Description: On the page the last Flag partial is found: JrFagL

Flag: {U25cs71YWJrFagL}

6: Command injection attack

Flag 6: Command injection flag = {RuRXA4i6dmJ4uwX}

Description: On the Wazuh dashboard, under Security Events, an alert appears: Suricata: Alert - EXTREMELY CRITICAL: Command Injection! Train #5344 is set to collide with Train #5566
Flag partial: U25

http://172.16.1.26:9000/index.html#!/login

Description: In Hive(SIEM), there's a case called Malicious Code Injection detection
Case # 9 - Train Command Injection
Flag partial: cs7

Description: In Hive(SIEM), open the tasks attached to the previous case and expand Shut down the train c&c system TODO: Consider this again
Flag partial: 1YW

Description: On the Wazuh Dashboard, in the alert an encrypted base64/rot13 string is found, decrypting this leads to:
SGFja2dyb3VwOiBGb25z // base64: Hackgroup: Fons TODO review name

https://gchq.github.io/CyberChef/

Flag partial: JrF

Description: Report the incident to the customer using the template found in TheHive
Flag partial: agL

Flag: {RuRXA4i6dmJ4uwX}