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 = {RDMkTx4ijxHZ0h8}
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: {RDMkTx4ijxHZ0h8}

2: Train entrance system

Flag 2: XSS flag = {0prbW5Whfp9wTOx}
Sub flags: 5

Sub flag: 1
Solution: On the Wazuh dashboard, under Security Events, an alert appears, open the event:

- *“Suricata: Alert - High Alert XSS attack deteced on Train entrance system(s)”*

Flag partial: {0pr
Important URL: http://172.16.1.26:9000/index.html#!/login

Sub flag: 2
Solution: In Hive(SIEM), there's a case called XSS attack detection - open the case and read the description

- *“Case #5 - XSS Attack alert”*

Flag partial: bW5
Important URL: http://172.16.1.26:9000/index.html#!/case/~~4328/details

Sub flag: 3
Solution: Open the tasks attached to the case, one of the tasks will mention:

- *“Visit the targeted page to scan inspect any possibility of defacements of the web page flag_2_partial_3=WhF”*

Flag partial: Whf
Important URL: http://172.16.1.26:9000/index.html#!/case/~~4328/tasks/~~12528

Sub flag: 4
Solution: Open the site found in the Wazuh Event (hostname + port + http.url)
Flag partial: p9w
Important URL: http://172.16.1.15:5002/vulnerabilities/xss_s/

Sub flag: 5
Description: The page has been griefed, go back to the Hive & open the customer contact form
Flag partial: T0x}
Important URL: http://172.16.1.26:9000/index.html#!/case/~~4328/tasks/~~12528

Flag: {0prbW5Whfp9wTOx}

3: Communication System Attack

Flag 3: CSRF flag = {Er4XCumRFhVEC0t}
Sub flags: 4

Sub flag: 1/4
Description: On the Wazuh dashboard, under Security Events, an alert appears:
Suricata: Alert - CRITICAL: Detected CSRF on Train entrance systems
Flag partial: {Er4
Important URL: http://172.16.1.26:9000/index.html#!/login

Sub flag: 2/4
Description: In Hive(SIEM), there's a case called CSRF detection - open the case and read the details/description
Case # 8 - CSRF Attack
Flag partial: XCu
Important URL: http://172.16.1.26:9000/index.html#!/case/~~40972376/details

Sub flag: 3/4
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: mRFh
Important URL: http://172.16.1.26:9000/index.html#!/case/~~40972376/tasks/~~32968

Sub flag: 4/4
Description: Execute a curl command on the IP-address found in Wazuh + endpoint like such:

- curl http://172.16.1.15/adminpanel/index.html

Flag partial: VEC0t}
Important URL: http://172.16.1.15/adminpanel/index.html

Flag: {Er4XCumRFhVEC0t}

4: Railway crossing Attack

Flag 4: Weak Session Id flag = {Fm1AyI1Y9QSH9yP}
Sub flags: 3

Sub flag: 1/3
Solution: On the Wazuh dashboard, under Security Events, an alert appears:

- *“Suricata: Alert - CRITICAL: Unauthorized Access Railway Crossing systems”*

Flag partial: {Fm1A
Important URL: http://172.16.1.15:5004/vulnerabilities/weak_id/

Sub flag: 2/3
Solution: On the docker dvwa on port 5400 the second partial can be found.
Flag partial: yI1Y9
Important URL: http://172.16.1.26:9000/index.html#!/login

Sub flag: 3/3
Solution: In Hive(SIEM), open the tasks attached to the previous case. Here can the flag be found.
Flag partial: QSH9yP}
Important URL: http://172.16.1.26:9000/index.html#!/case/~~4136/tasks/~~4112

Flag: {Fm1AyI1Y9QSH9yP}

5: Speedup/jam attack

Flag 5: Javascript flag = {U25cs71YWJrFagL}
Sub flags: 4

Sub flag: 1/4
Solution: 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
Important URL: http://172.16.1.26:9000/index.html#!/login

Sub flag: 2/4
Solution: In Hive(SIEM), there's a case called Javascript attack - Speedup/jam
Case # 11 - Javascript attack - Speedup/jam
Flag partial: cs7
Important URL: http://172.16.1.26:9000/index.html#!/case/~~40964304/details

Sub flag: 3/4
Solution: In Hive(SIEM), open the tasks page and you see a flag between the tasks.
Flag partial: 1YW
Important URL: http://172.16.1.26:9000/index.html#!/case/~~20520/tasks/~~16488

Sub flag: 4/4
Solution: On the page is the last Flag partial.
Flag partial: JrFagL}
Important URL: http://172.16.1.15:5005/vulnerabilities/javascript/

Flag: {U25cs71YWJrFagL}

6: Command injection attack

Flag 6: Injection flag = {RuRXA4i6dmJ4uwX}
Sub flags: 6

Sub flag: 1/6
Solution: 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: {RuR
Important URL: http://172.16.1.26:9000/index.html#!/login

Sub flag: 2/6
Solution: On the Wazuh dashboard, in the security event a base64 string appears, decoding it leads to:

- *“we_are_legion_flag_6_partial_2=XA4”*

Flag partial: XA4
Important URL: https://www.base64decode.org/

Sub flag: 3/6
Solution: In Hive(SIEM), there's a case called Malicious Code Injection detection / Collision prevention system
Case # 9 - Train Command Injection
Flag partial: i6d
Important URL: http://172.16.1.26:9000/index.html#!/case/~~40964304/details

Sub flag: 4/6
Solution: In Hive(SIEM), open the task contact customer
Immediately contact customer using a template
Flag partial: mJ
Important URL: http://172.16.1.26:9000/index.html#!/case/~~40964304/tasks/~~24616

Sub flag: 5/6
Solution: On the Wazuh Dashboard, open the URL in the security alert
In the train collusion tab the 5th partial is revealed:
Flag partial: 4u
Important URL: http://172.16.1.15:5006/vulnerabilities/exec/

Sub flag: 6/6
Solution: Decode the base64 string found in the same page
In the train colusion tab the 5th partial is revealed:
we_are_legion_flag_6_final: wX}
Important URLS:

- http://172.16.1.15:5006/vulnerabilities/exec/
- https://gchq.github.io/CyberChef/

Flag: {RuRXA4i6dmJ4uwX}