NICE Challenge Project

Challenge Submission Report

Submission ID: 73042

Timestamp: 8/14/2022 8:45 AM UTC

Name: Richard Compton

Challenge ID: 79

Challenge Title: Properly Prioritized Web Watching

Scenario

Jan Cortes and Tim Clark have been dedicating too much time to support tickets for the website being broken. We can't make it work on every browser, so we need you to watch the traffic to our website so we know which web browsers to dedicate time to supporting.
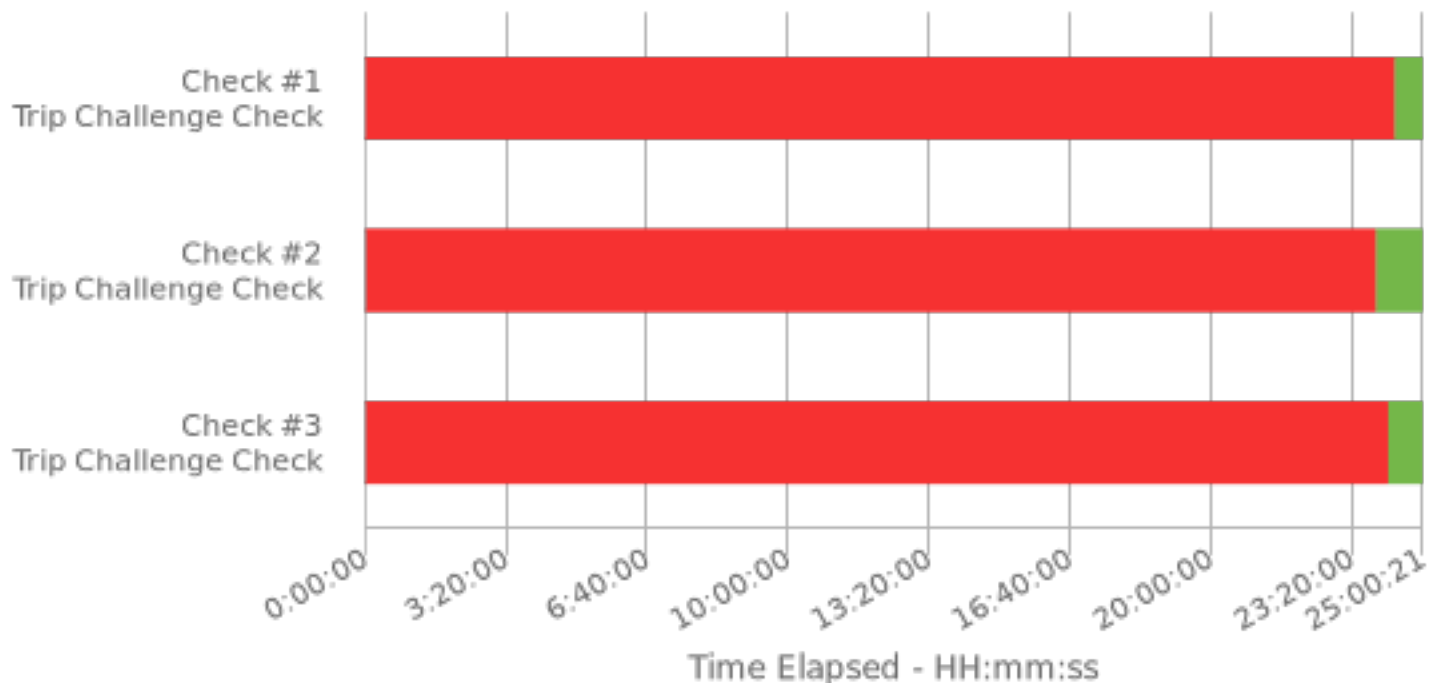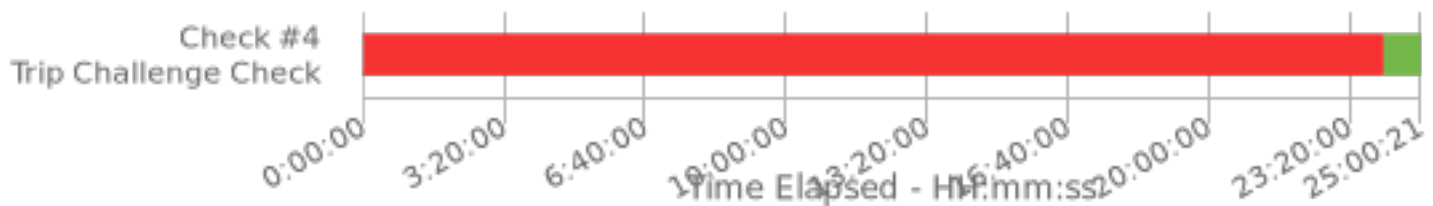
Duration

25:00

Full Check Pass

Full: 4/4

Final Check Details

- ✅ Check #1: Connection One Information Correct
- ✅ Check #2: Connection Two Information Correct
- ✅ Check #3: Connection Three Information Correct
- ✅ Check #4: Connection Four Information Correct

Specialty Area

Cybersecurity Defense Analysis

Work Role

Cyber Defense Analyst

NICE Framework Task

T0297 Identify applications and operating systems of a network device based on network traffic.

Knowledge, Skills, and Abilities

• A0159 Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).

• K0001 Knowledge of computer networking concepts and protocols, and network security methodologies.

• K0058 Knowledge of network traffic analysis methods.

• K0060 Knowledge of operating systems.

• K0061 Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).

• K0111 Knowledge of network tools (e.g., ping, traceroute, nslookup)

• K0221 Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).

• K0301 Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).

• S0156 Skill in performing packet-level analysis.

Centers of Academic Excellence Knowledge Units

• Basic Cyber Operations
• Basic Networking
• Network Forensics
• Operating Systems Concepts