NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/56787-15F7-C2080/

Submission ID: 62256

Timestamp: 1/29/2022 3:43 PM UTC

Name: Winston Lee

Challenge ID: 116

Challenge Title: Dangerous Drives [NG]

Scenario

A USB thumb drive of unknown origin or owner has been found in the office. I need you to check and verify that the thumb drive does not contain any malicious software that could infect and damage the company's valuable data.

Reviewed By: Solomon Zewde at Houston Community College

Duration

1:31

Full Check Pass

Full: 8/8

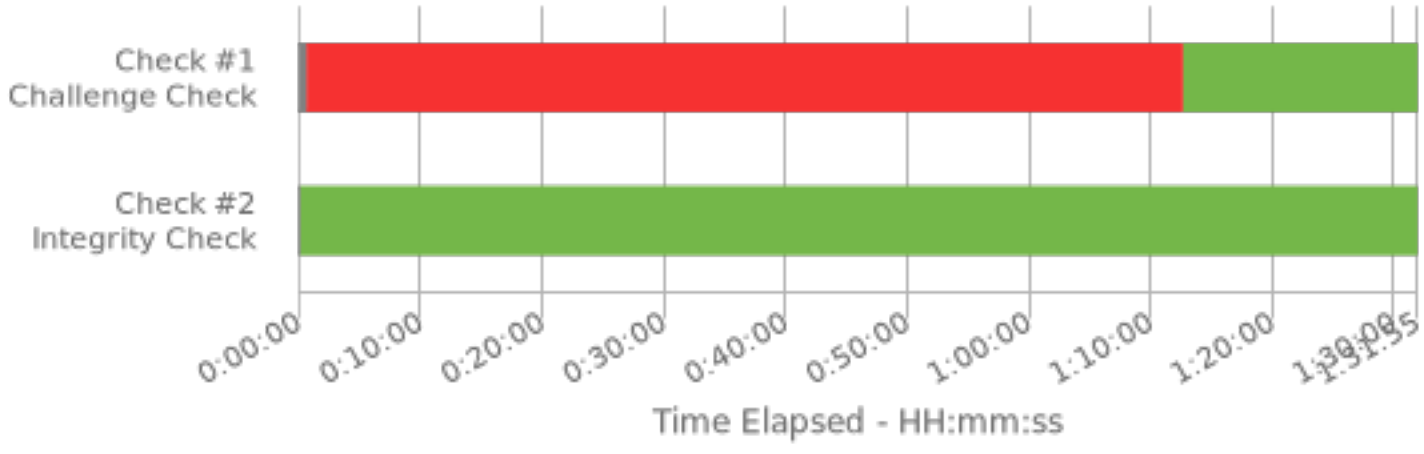
Final Check Details

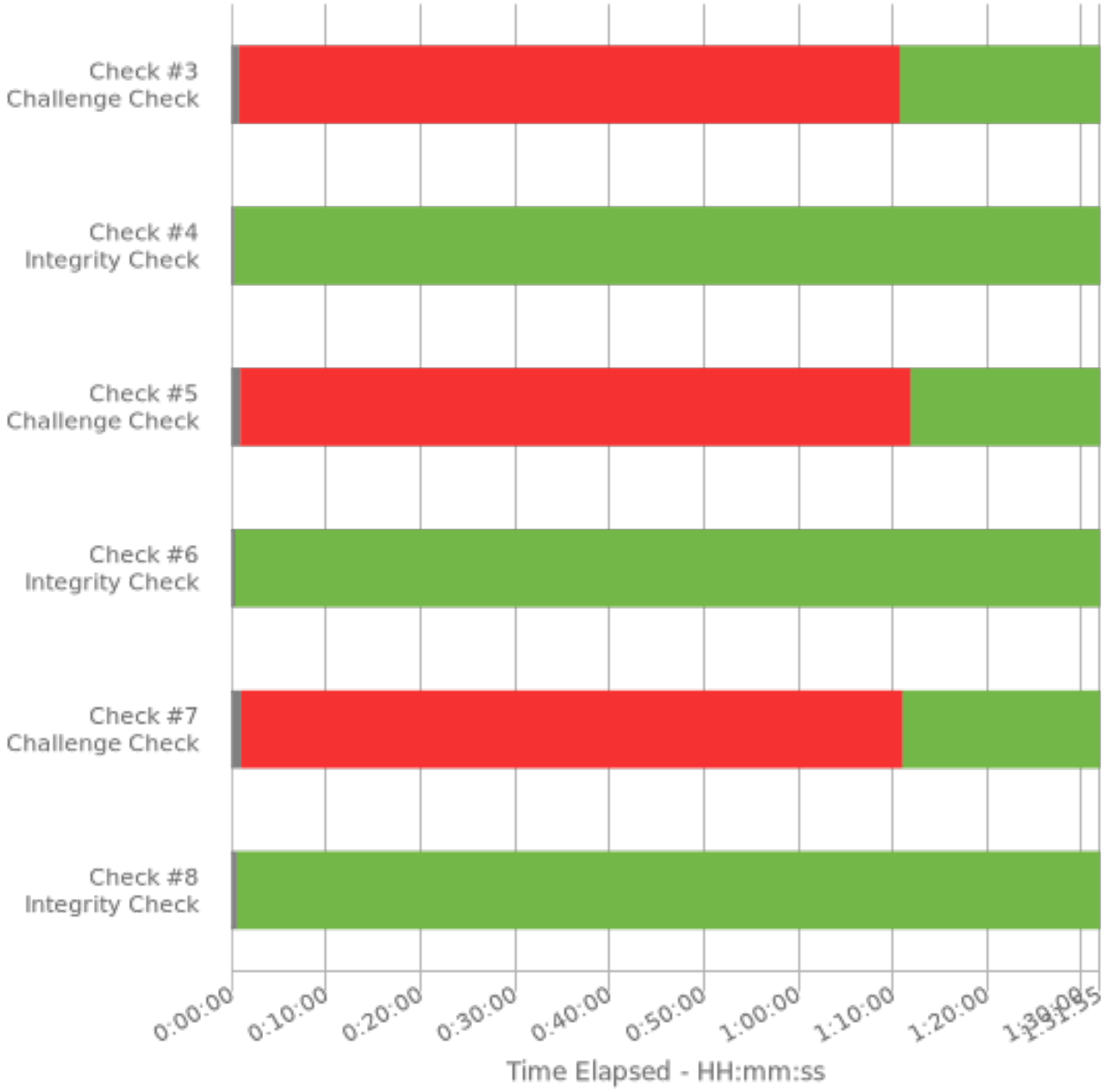
- Check #1: Remove Infected File No.1
- Check #2: Maintain File Integrity No.1 [Should be green]
- Check #3: Remove Infected File No.2
- Check #4: Maintain File Integrity No.2 [Should be green]
- Check #5: Remove Infected File No.3
- Check #6: Maintain File Integrity No.3 [Should be green]
- Check #7: Remove Infected File No.4
- Check #8: Maintain File Integrity No.4 [Should be green]

Curator Feedback

Challenge Attempt Successful: ✔

Successful troubleshooting with good documentation.





Specialty Area

Digital Forensics

Work Role

Law Enforcement/CounterIntelligence Forensics

NICE Framework Task

T0285 Perform virus scanning on digital media.

Knowledge, Skills, and Abilities

• K0017 Knowledge of concepts and practices of processing digital forensic data.

• K0060 Knowledge of operating systems.

• K0117 Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).

• K0132 Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.

• K0133 Knowledge of types of digital forensics data and how to recognize them.

• K0187 Knowledge of file type abuse by adversaries for anomalous behavior.

• S0067 Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).

• S0073 Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).

• S0092 Skill in identifying obfuscation techniques.

Centers of Academic Excellence Knowledge Units

• Cybersecurity Foundations

• Cybersecurity Principles

• Cyber Threats

• Intrusion Detection/Prevention Systems

• Operating Systems Concepts

• Vulnerability Analysis