NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/FD120-48FF-331A8/

Submission ID: 64406

Timestamp: 2/20/2022 4:36 PM UTC

Name: Frankie Lopez

Challenge ID: 123

Challenge Title: Volatile Vulnerabilities [NG]

This report has not been published by a curator. The NICE Challenge Project cannot vouch for its accuracy.

Scenario

I have recently been notified of a security risk regarding two of our primary applications. These Applications, one for Human Resources and the other for Accounting, are installed on our machines as part of the base image we deploy. From what I've gathered, anyone from either group can launch either application and use the information the applications have access to maliciously. I need you to get on it before the vulnerability is realized and exploited.

Duration

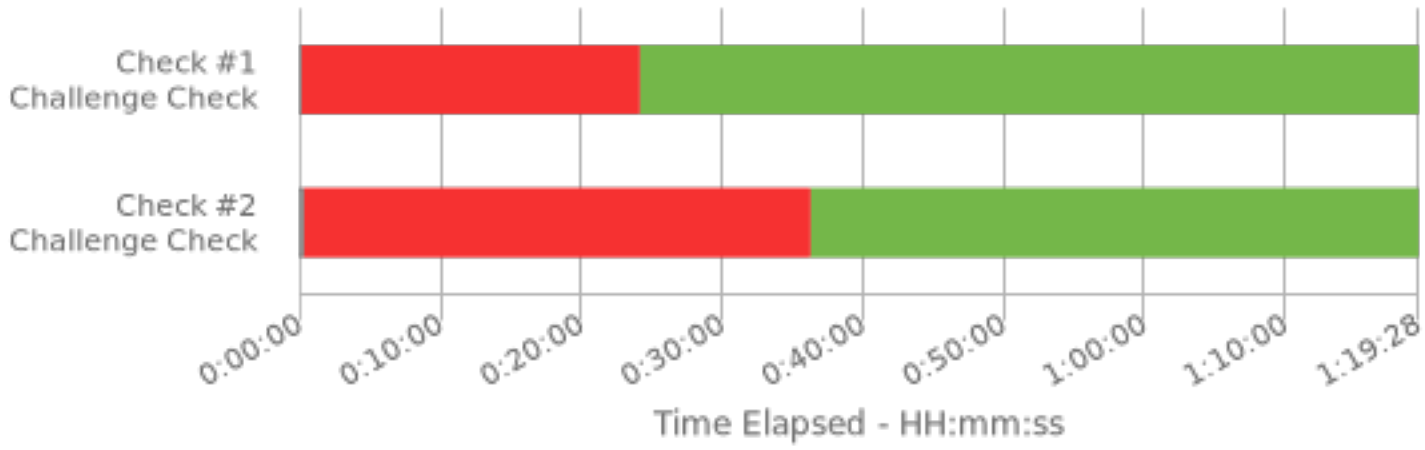
1:19

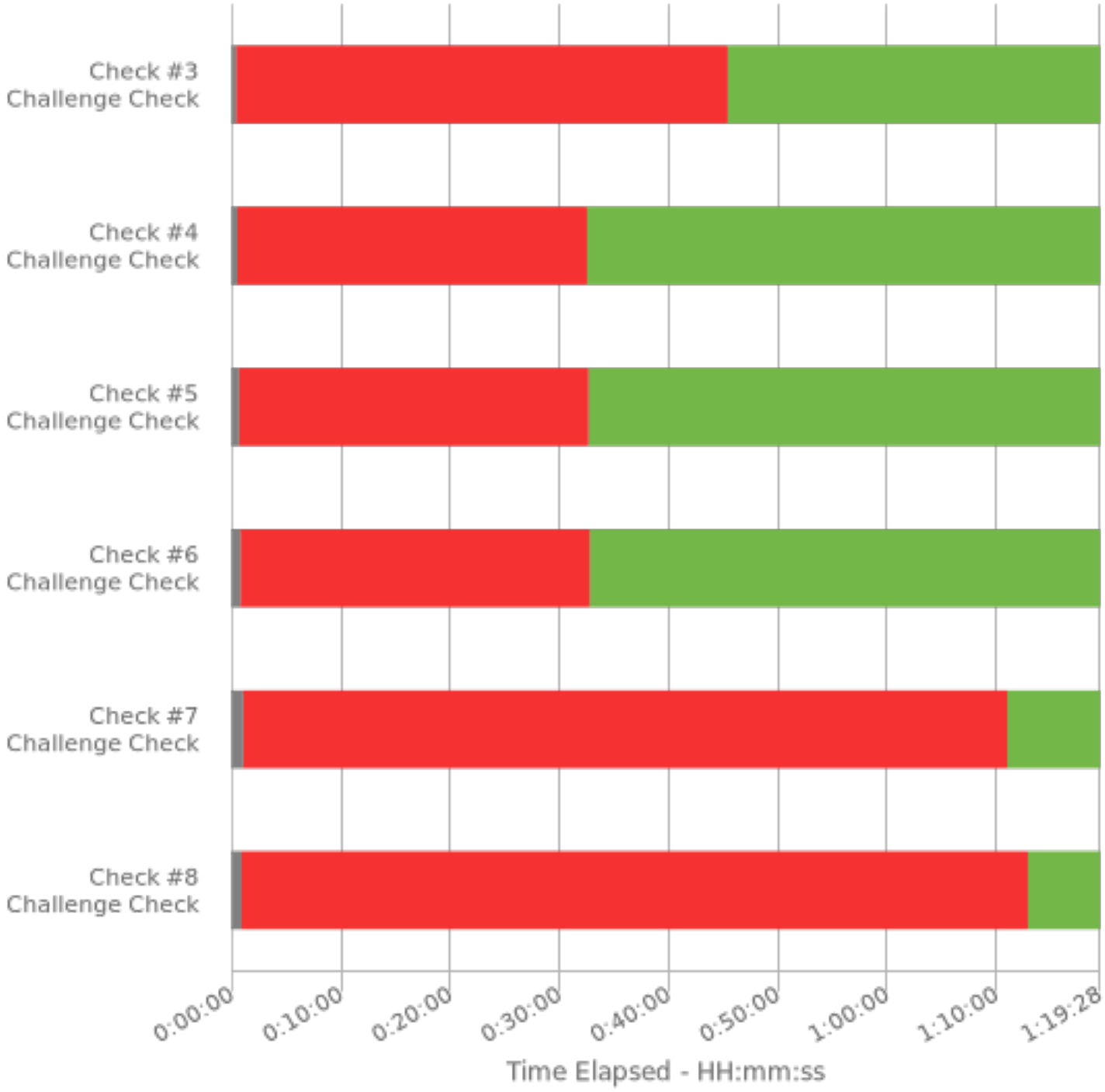
Full Check Pass

Full: 8/8

Final Check Details

- Check #1: DasApp GPO Created and Linked at Domain Level and Enforced
- Check #2: Enable Application Identification Service in DasApp Policy
- Check #3: Enable Executable Enforcment on AppLocker in DasApp Policy
- Check #4: Generate Default AppLocker Rule No.1 in DasApp Policy
- Check #5: Generate Default AppLocker Rule No.2 in DasApp Policy
- Check #6: Generate Default AppLocker Rule No.3 in DasApp Policy
- Check #7: Use AppLocker to Deny HR from Accounting Application
- Check #8: Use AppLocker to Deny Accounting from HR Application





Specialty Area

Systems Analysis

Work Role

Systems Security Analyst

NICE Framework Task

T0123 Implement specific cybersecurity countermeasures for systems and/or applications.

Knowledge, Skills, and Abilities

- K0004 Knowledge of cybersecurity and privacy principles.
- K0005 Knowledge of cyber threats and vulnerabilities.
- K0036 Knowledge of human-computer interaction principles.
- K0040 Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
- K0044 Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- K0049 Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
- K0060 Knowledge of operating systems.
- K0276 Knowledge of security management.
- K0297 Knowledge of countermeasure design for identified security risks.
- S0001 Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
- S0031 Skill in developing and applying security system access controls.
- S0147 Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).

Centers of Academic Excellence Knowledge Units

- Cybersecurity Foundations
- IT Systems Components
- Operating Systems Concepts
- Operating Systems Hardening
- Windows System Administration