# NICE Challenge Project

## Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/4AC94-2967-746E3/

Submission ID: 114476

Timestamp: 6/4/2024 12:41 AM UTC

Name: Colin Choquette

Challenge ID: 80

Challenge Title: Unauthorized Activity Alert

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

### Scenario

The network firewall has been compromised, and the overall system security of each host is not guaranteed. We need you to assess each host, implementing security improvements and configuration changes to assure system integrity.

### Duration

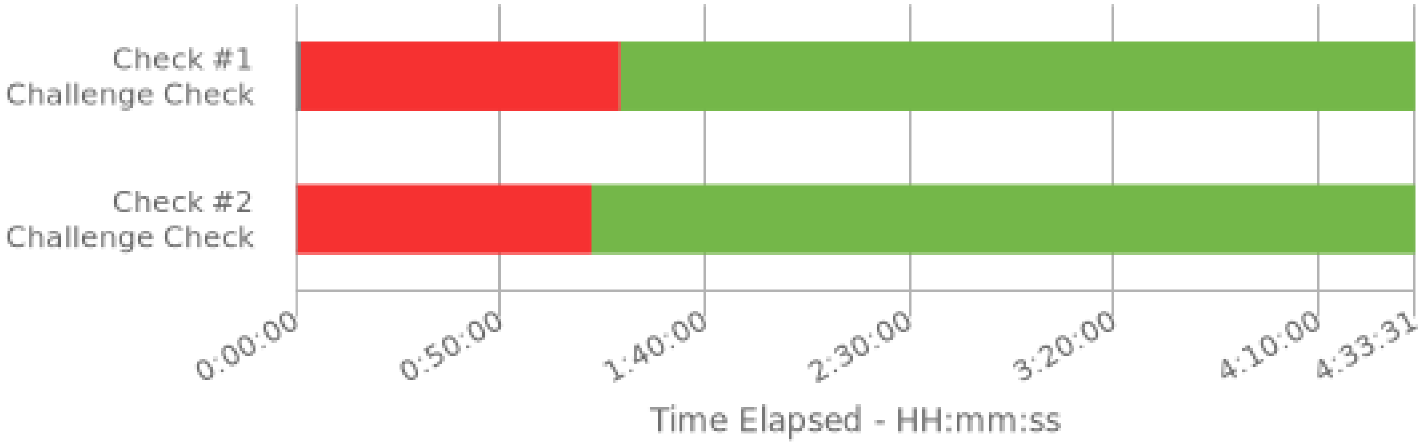
4:33

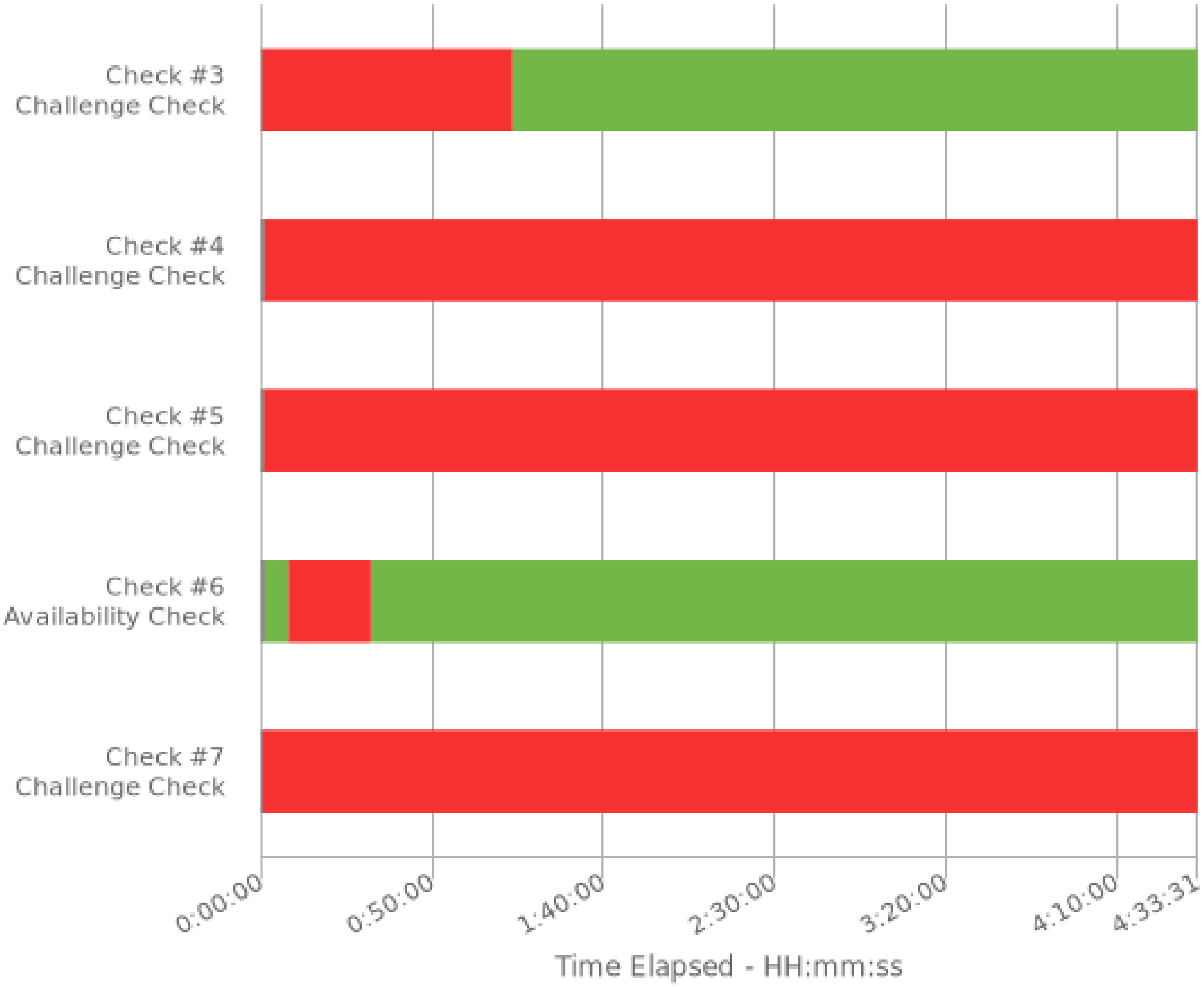
### Full Check Pass

Partial: 4/7

### Final Check Details

- ✓ Check #1: Workstation Remote Desktop and Firewall in Correct State
- ✓ Check #2: Database Remote Desktop and Firewall in Correct State
- ✓ Check #3: Domain Controller Remote Desktop and Firewall in Correct State
- ✗ Check #4: Prod-Joomla Unauthorized User Access Revoked
- ✗ Check #5: Linux Firewalls Up
- ✓ Check #6: Web Server and Database Operational [Should Start Green]
- ✗ Check #7: Environment Protected Against Future Malicious Activity [Approx Three Minute Refresh]





## Specialty Area

Cybersecurity Defense Analysis

## Work Role

Cyber Defense Analyst

## NICE Framework Task

T0504 Assess and monitor cybersecurity related to system implementation and testing practices.

## Knowledge, Skills, and Abilities

- A0123 Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- K0001 Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0005 Knowledge of cyber threats and vulnerabilities.
- 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).
- K0167 Knowledge of system administration, network, and operating system hardening techniques.
- S0027 Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
- S0367 Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

## Centers of Academic Excellence Knowledge Units

- Cybersecurity Foundations
- Network Defense
- Network Security Administration
- Operating Systems Administration
- Operating Systems Hardening