NICE Challenge Project

Challenge Submission Report

Submission ID: 95132

Timestamp: 9/29/2023 2:43 PM UTC

Name: Jordan Calvert

Challenge ID: 167

Challenge Title: Operations Gone Wrong: The Incompetent Intern [NG]

Scenario

We had one of our interns perform various tasks on a few of our systems such as the database and ftp server and unfortunately, everything that was done ignored our standard operating procedures and now we have multiple major services such as ftp and ssh left in vulnerable states. We need these services fixed to comply with our organizational standard operating procedures. Other admins will relay to you the required standards regarding any misconfigured services they have noticed.
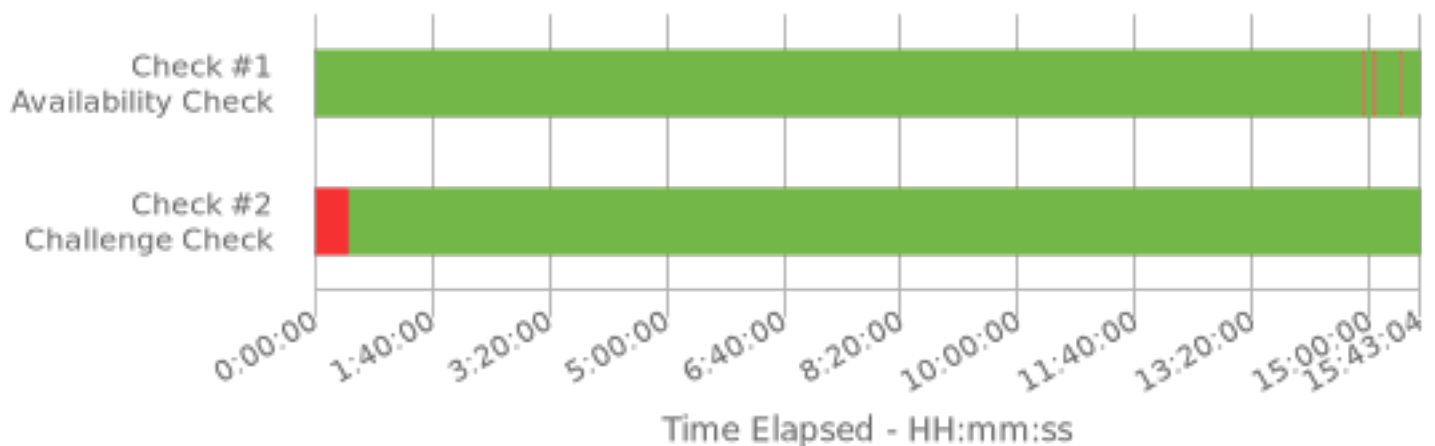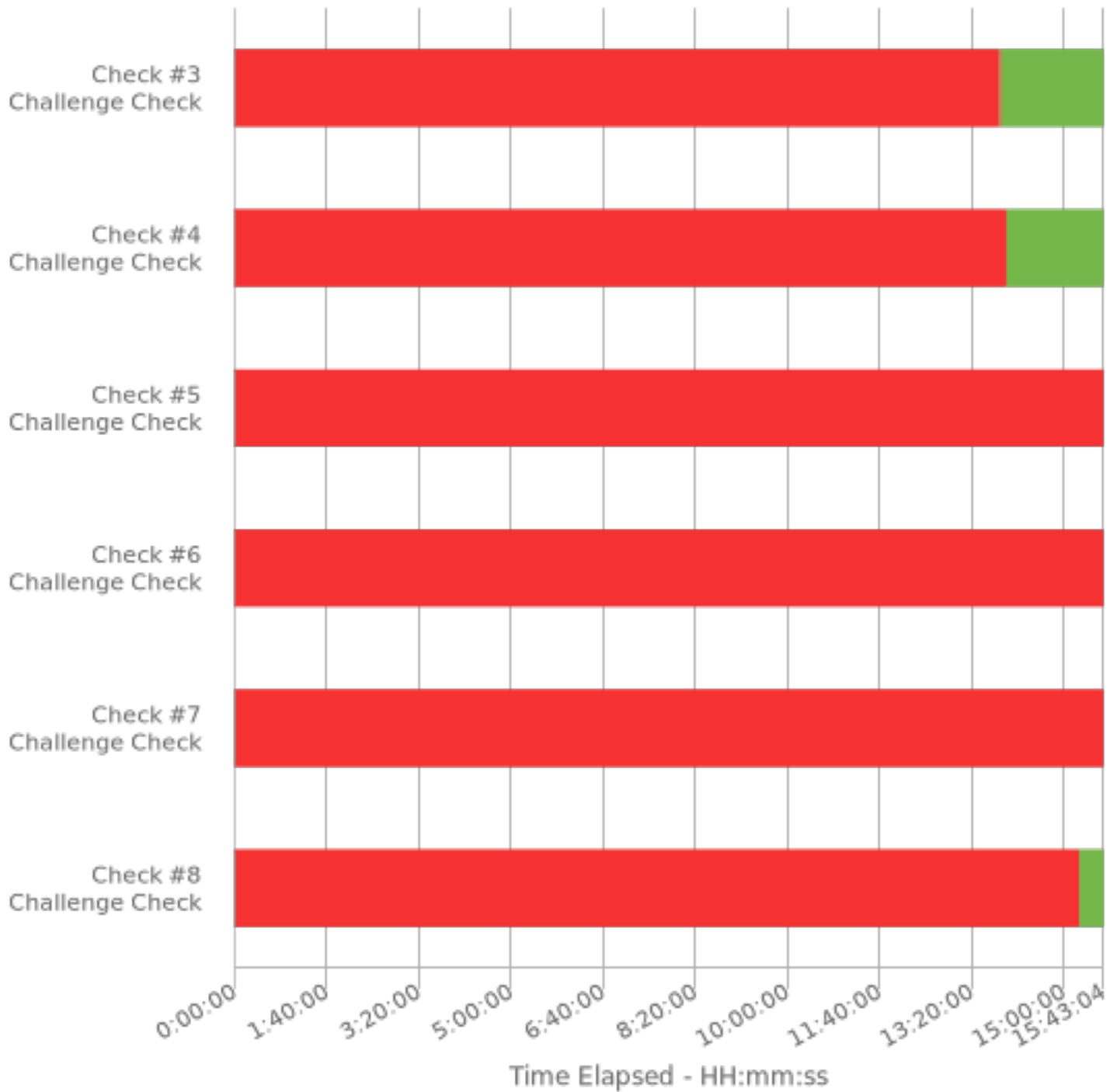
Duration

15:43

Full Check Pass

Partial: 5/8

Final Check Details

- ✅ Check #1: Check for selinux on Prod-Web - Should stay Green
- ✅ Check #2: Prod-Web Website Functionality Restored
- ✅ Check #3: Require thanh to Use a Password to sudo on Dev-Web
- ✅ Check #4: Require gthatcher to Use a Password to sudo on Dev-Web
- ❌ Check #5: Forbid Mysql remote root login on Database
- ❌ Check #6: Forbid Anonymous FTP Login on Fileshare
- ❌ Check #7: Forbid SSH User Login SSHLOGIN on Prod-Web
- ✅ Check #8: Forbid SSH User Login ROOT on Prod-Web

Time Elapsed - HH:mm:ss

Time Elapsed - HH:mm:ss

Specialty Area

Systems Administration

Work Role

System Administrator

NICE Framework Task

T0458 Comply with organization systems administration standard operating procedures.

Knowledge, Skills, and Abilities

• K0004 Knowledge of cybersecurity and privacy principles.

• K0005 Knowledge of cyber threats and vulnerabilities.

• K0006 Knowledge of specific operational impacts of cybersecurity lapses.

• K0053 Knowledge of measures or indicators of system performance and availability.

• K0077 Knowledge of server and client operating systems.

• K0088 Knowledge of systems administration concepts.

• K0158 Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).

• K0167 Knowledge of system administration, network, and operating system hardening techniques.

• K0318 Knowledge of operating system command-line tools.

• S0143 Skill in conducting system/server planning, management, and maintenance.

• S0151 Skill in troubleshooting failed system components (i.e., servers)

• S0153 Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems.

• S0158 Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).

Centers of Academic Excellence Knowledge Units

• IT Systems Components
• Operating Systems Administration
• Operating Systems Concepts