



NICE Challenge Project

Challenge Submission Report

<https://portal.nice-challenge.com/reports/verify/5C03E-3ED1-8D810/>

Submission ID: 77824

Timestamp: 11/11/2022 9:55 PM UTC

Name: Harsha Siddapura Gnaneshwara Harsha Siddapura Gnaneshwara

Challenge ID: 76

Challenge Title: Firewall Update: Tables for Two



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

Scenario

The way firewalls in Linux are implemented is changing. We need you to make sure our Linux boxes are keeping up with those changes so that we don't create any problems for ourselves in the future.

Duration

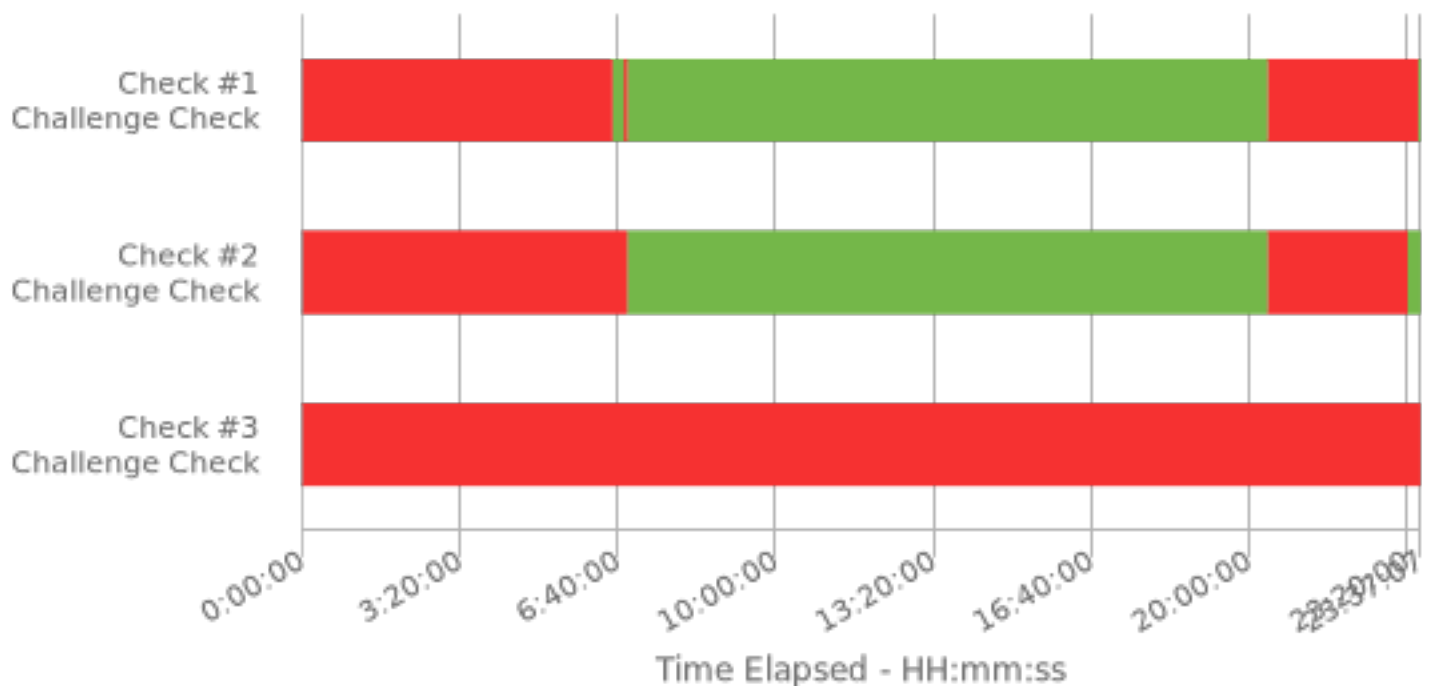
23:37

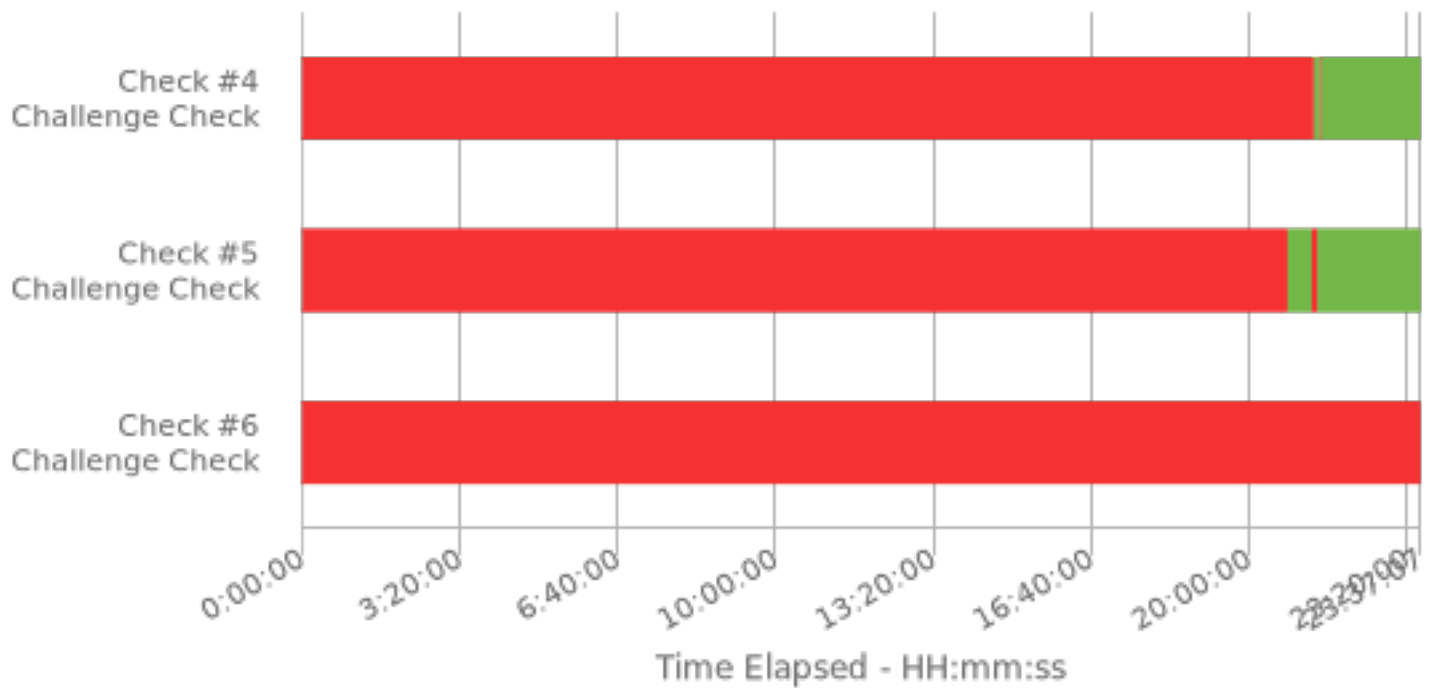
Full Check Pass

Partial: 4/6

Final Check Details

- ✓ Check #1: Security-Desk iptables Uninstalled
- ✓ Check #2: Security-Desk nftables Service Enabled
- ✗ Check #3: Security-Desk Filtering Traffic Correctly
- ✓ Check #4: Prod-Joomla iptables Uninstalled
- ✓ Check #5: Prod-Joomla nftables Service Enabled
- ✗ Check #6: Prod-Joomla Filtering Traffic Correctly





Specialty Area

Cybersecurity Defense Infrastructure Support

Work Role

Cyber Defense Infrastructure Support Specialist

NICE Framework Task

T0180 Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.

Knowledge, Skills, and Abilities

- K0001 Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0004 Knowledge of cybersecurity and privacy principles.
- 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]).
- K0179 Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0205 Knowledge of basic system, network, and OS hardening techniques.
- S0121 Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).
- 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

- Basic Networking
- Cybersecurity Principles

- IT Systems Components
- Linux System Administration
- Network Defense
- Network Security Administration
- Network Technology and Protocols