NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/5AF56-EA94-C61FC/

Submission ID: 98606

Timestamp: 11/4/2023 10:21 PM UTC

Name: Kavita Kamtekar

Challenge ID: 63

Challenge Title: Foolish Firewall Configurations

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

Scenario

An intern of ours installed a new core firewall about a month ago. A recent network security audit has shown that, while being installed, the new firewall was not properly configured. Additionally, three of our server's host firewalls have not been configured to filter inbound traffic properly. You are tasked with configuring the firewalls on each ill-configured host as well as the core firewall to reject all but necessary traffic.

Duration

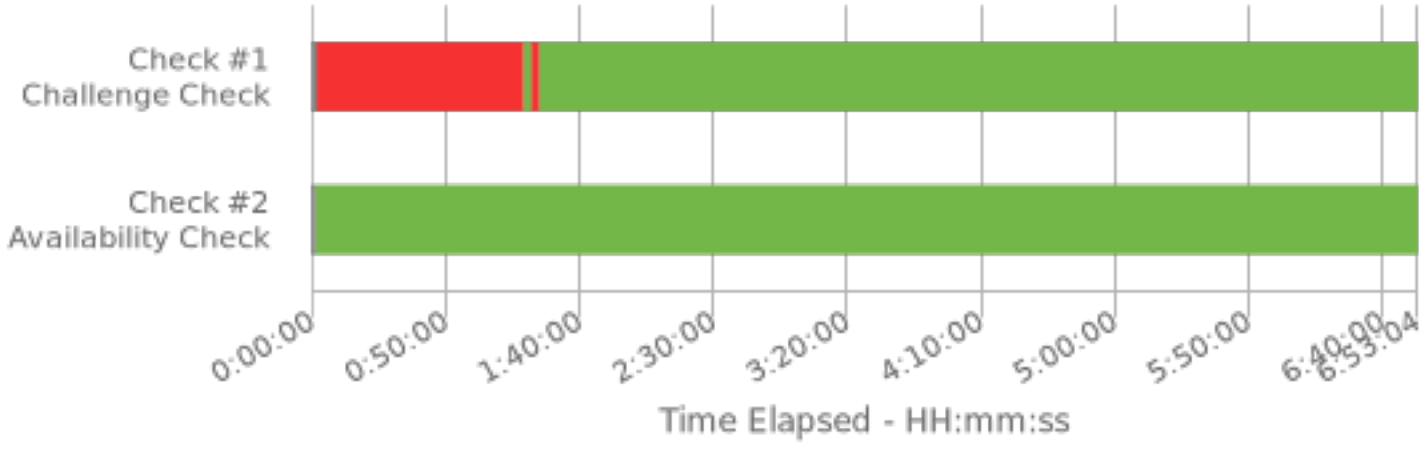
6:53

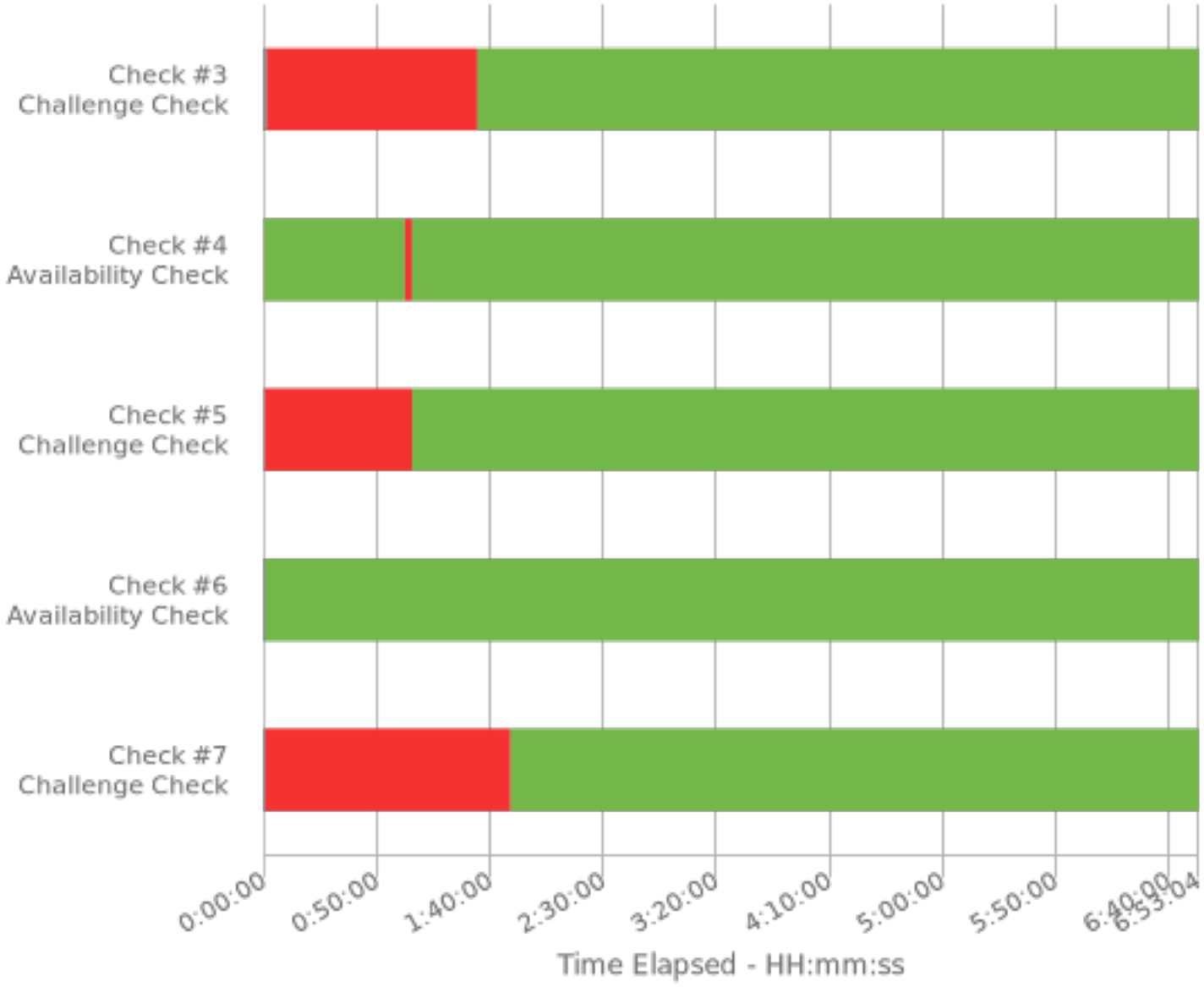
Full Check Pass

Full: 7/7

Final Check Details

- Check #1: Network firewall only allows external HTTP and HTTPS traffic to Prod-Joomla [Approx. 2m Refresh]
- Check #2: Prod-Joomla has HTTP HTTPS and SSH available via host firewall [Should Stay Green]
- Check #3: Prod-Joomla only has HTTP HTTPS and SSH available via host firewall
- Check #4: Database has MySQL available via host firewall [Should Stay Green]
- Check #5: Database only has MySQL available via host firewall
- Check #6: Fileshare has SFTP and Samba available via host firewall [Should Stay Green]
- Check #7: Fileshare only has SFTP and Samba available via host firewall





Specialty Area

Cybersecurity Defense Infrastructure Support

Work Role

Cyber Defense Infrastructure Support Specialist

NICE Framework Task

T0438 Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).

Knowledge, Skills, and Abilities

• K0001 Knowledge of computer networking concepts and protocols, and network security methodologies.

• K0004 Knowledge of cybersecurity and privacy principles.

• K0005 Knowledge of cyber threats and vulnerabilities.

• K0033 Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).

• K0044 Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

• K0221 Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).

• K0332 Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.

• S0007 Skill in applying host/network access controls (e.g., access control list).

• S0121 Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).

Centers of Academic Excellence Knowledge Units

• Cybersecurity Foundations

• Cybersecurity Principles

• Network Defense

• Network Security Administration

• Operating Systems Administration

• Operating Systems Concepts