NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/7826D-B30C-0C6D2/

Submission ID: 92696

Timestamp: 9/1/2023 2:44 AM UTC

Name: Joshua Kisner

Challenge ID: 129

Challenge Title: Interns & HR on the Domain Controller [NG]

Scenario

Recently we concluded our first intern program here at DASWebs. While we expected it to be valuable to the intern, Rob, after working with our techs for a while on our network he brought to our attention that he could access critical systems with his basic domain credentials. After which we reviewed how things were setup we found that many domain users have access to servers and shares they shouldn't. The techs and I have already outlines the basic start to fixing these issues and we want you to handle it.

Reviewed By: Solomon Zewde at Houston Community College

Duration

1:17

Full Check Pass

Full: 7/7

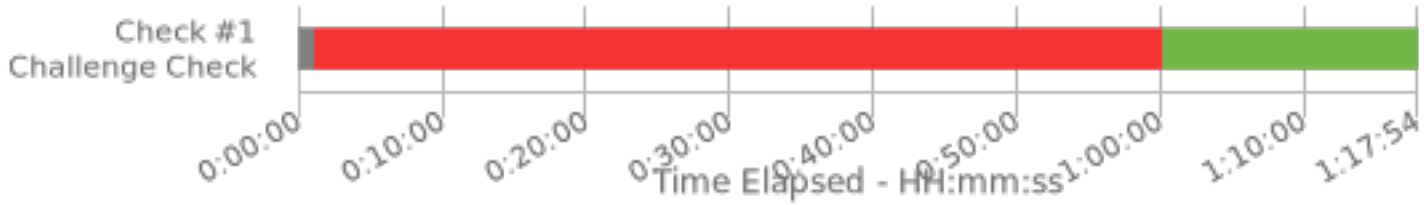
Final Check Details

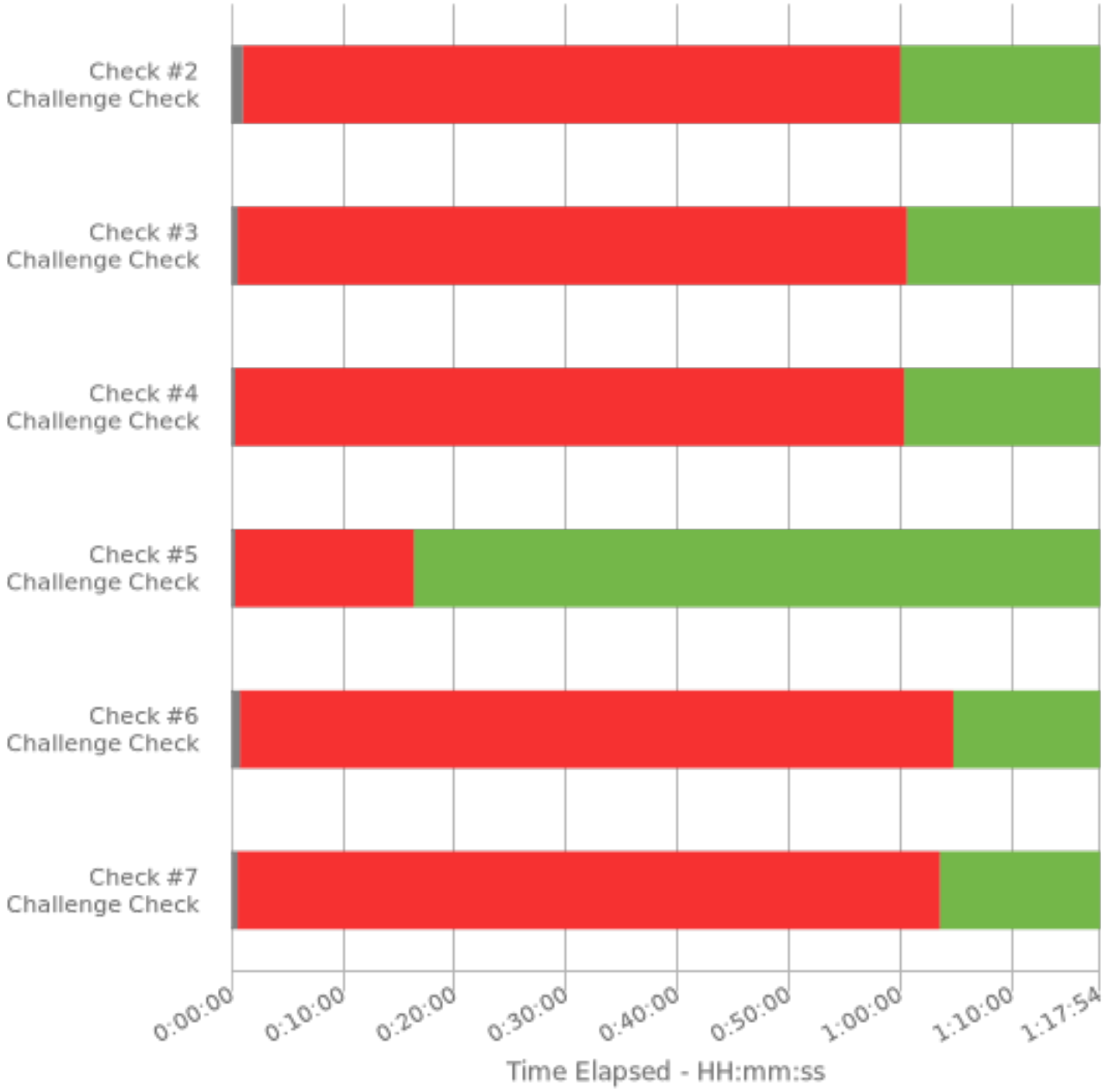
- Check #1: HR Share access granted to only Sergio via HRSec security group
- Check #2: HR Share access Restricted to Domain Admins security group
- Check #3: Accounting Share access granted to only Brimlock via AccountingSec security group
- Check #4: Accounting Share access Restricted to Domain Admins security group
- Check #5: Robs Account Disabled
- Check #6: Brimlock Stones can only log onto Workstation-Desk
- Check #7: Sergio Chanel can only log onto Workstation-Desk

Curator Feedback

Challenge Attempt Successful: ✔

Well done!





Specialty Area

Systems Administration

Work Role

System Administrator

NICE Framework Task

T0144 Manage accounts, network rights, and access to systems and equipment.

Knowledge, Skills, and Abilities

- K0002 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- K0004 Knowledge of cybersecurity and privacy principles.
- K0005 Knowledge of cyber threats and vulnerabilities.
- K0049 Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
- K0077 Knowledge of server and client operating systems.
- K0088 Knowledge of systems administration concepts.
- K0100 Knowledge of the enterprise information technology (IT) architecture.
- 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.
- S0016 Skill in configuring and optimizing software.
- S0043 Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).
- S0143 Skill in conducting system/server planning, management, and maintenance.
- 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

- Cybersecurity Foundations
- Cybersecurity Principles
- Operating Systems Concepts
- Windows System Administration

NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/F2FE6-8218-3BC43/

Submission ID: 92699

Timestamp: 9/1/2023 3:16 AM UTC

Name: Joshua Kisner

Challenge ID: 115

Challenge Title: Helpdesk Fun: User Workstation Nightmares [NG]

Scenario

One of our accountants, Sergio Chanel, has been having several issues with his Windows workstation lately. The issues have gotten so bad that he is now unable to complete his work in a timely manner. You will need to review his Windows workstation profile and fix the issues he has reported as well as restore any basic company default settings the other IT staff request.

Reviewed By: Solomon Zewde at Houston Community College

Duration

0:12

Full Check Pass

Full: 5/5

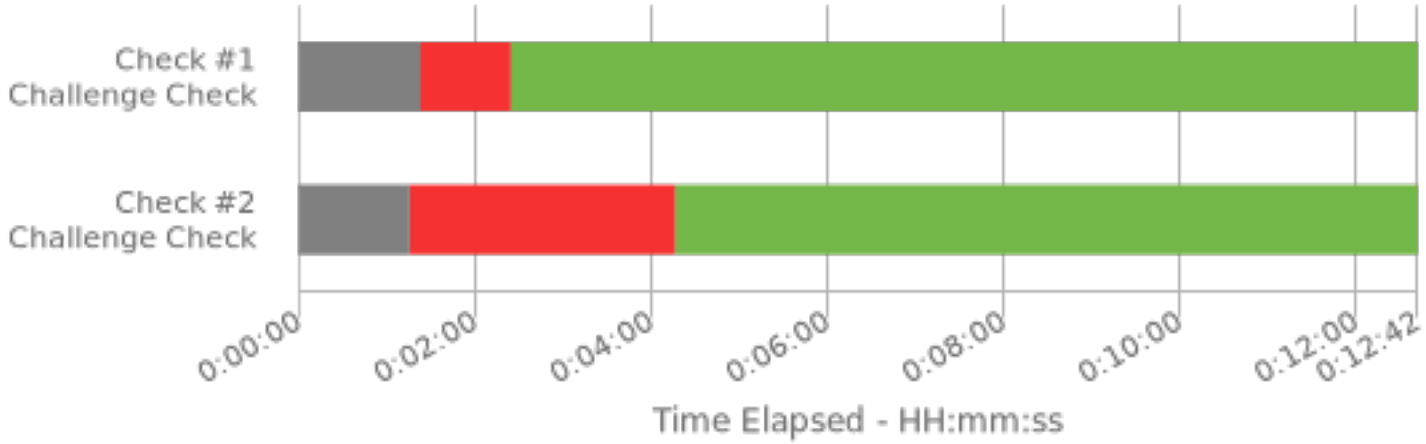
Final Check Details

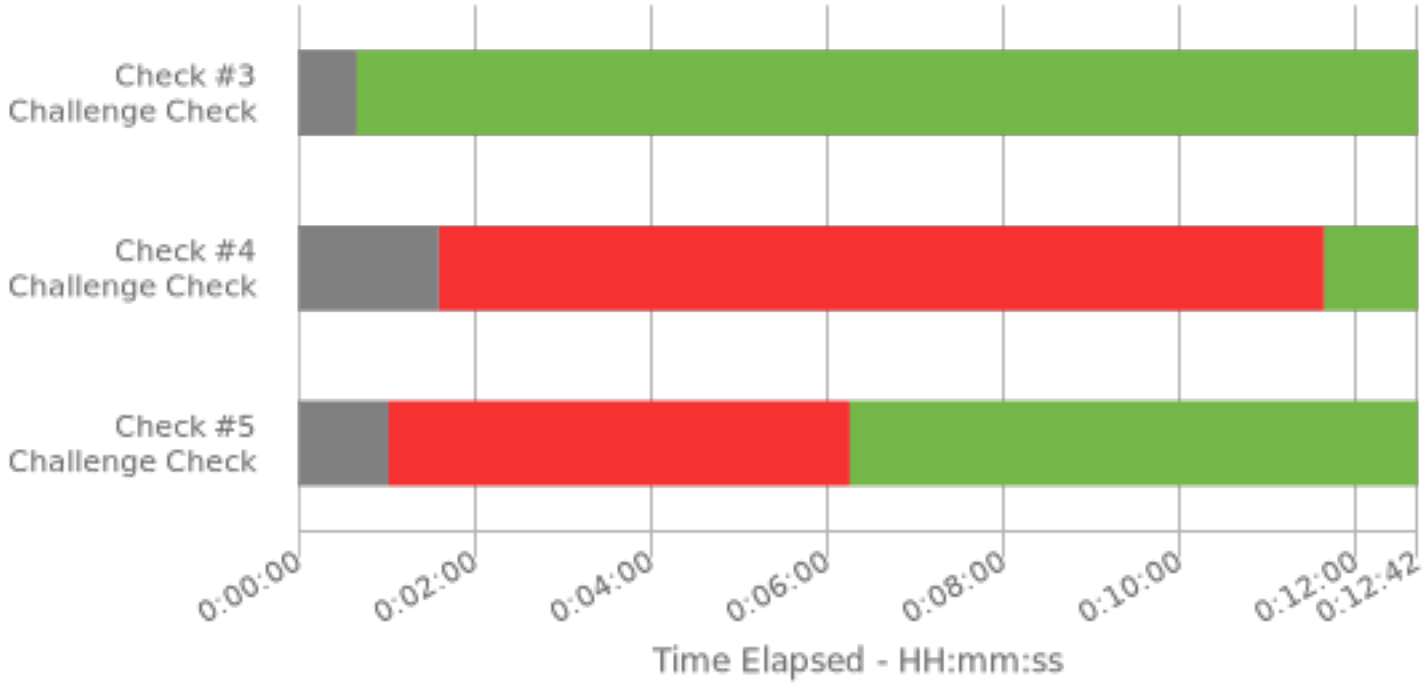
- Check #1: Fix Mouse Buttons
- Check #2: Fix Desktop Icons
- Check #3: Logged in as Sergio Chanel [Should Stay Green]
- Check #4: Fix The Internet
- Check #5: HR Network Share Mapped to Drive Letter H

Curator Feedback

Well done!

Challenge Attempt Successful: ✔





Specialty Area

Customer Service and Technical Support

Work Role

Technical Support Specialist

NICE Framework Task

T0468 Diagnose and resolve customer reported system incidents, problems, and events.

Knowledge, Skills, and Abilities

- K0088 Knowledge of systems administration concepts.
- K0292 Knowledge of the operations and processes for incident, problem, and event management.
- K0294 Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.
- K0302 Knowledge of the basic operation of computers.
- K0330 Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.
- S0058 Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.
- S0142 Skill in conducting research for troubleshooting novel client-level problems.
- S0159 Skill in configuring and validating network workstations and peripherals in accordance with approved standards and/or specifications.

Centers of Academic Excellence Knowledge Units

- IT Systems Components
- Operating Systems Concepts

NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/D0A18-91FF-28505/

Submission ID: 92944

Timestamp: 9/5/2023 2:17 AM UTC

Name: Joshua Kisner

Challenge ID: 116

Challenge Title: Dangerous Drives [NG]

Scenario

A USB thumb drive of unknown origin or owner has been found in the office. I need you to check and verify that the thumb drive does not contain any malicious software that could infect and damage the company's valuable data.

Reviewed By: Solomon Zewde at Houston Community College

Duration

0:12

Full Check Pass

Full: 8/8

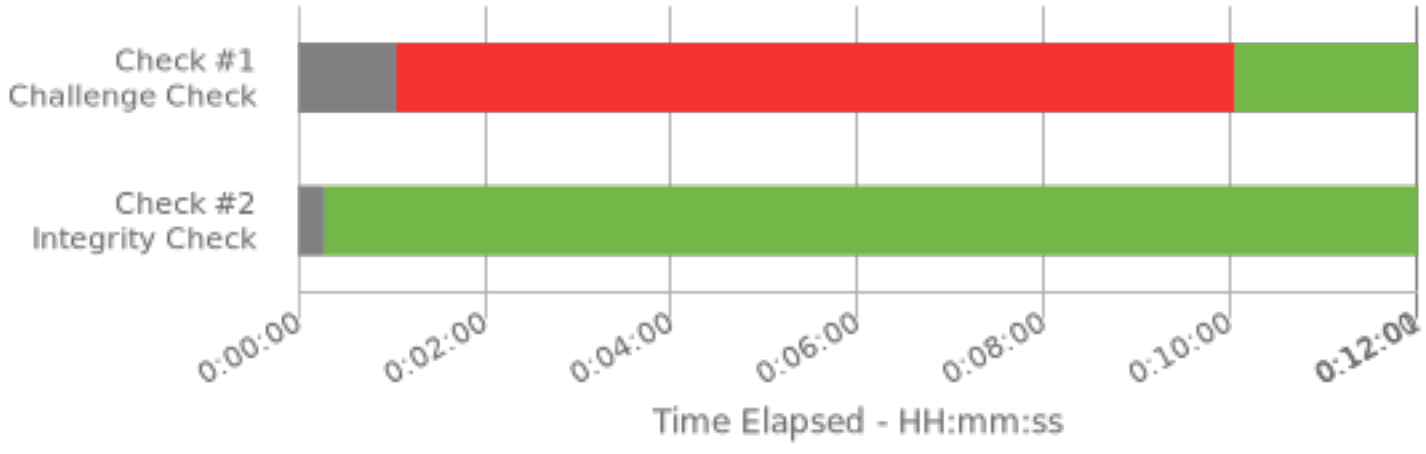
Final Check Details

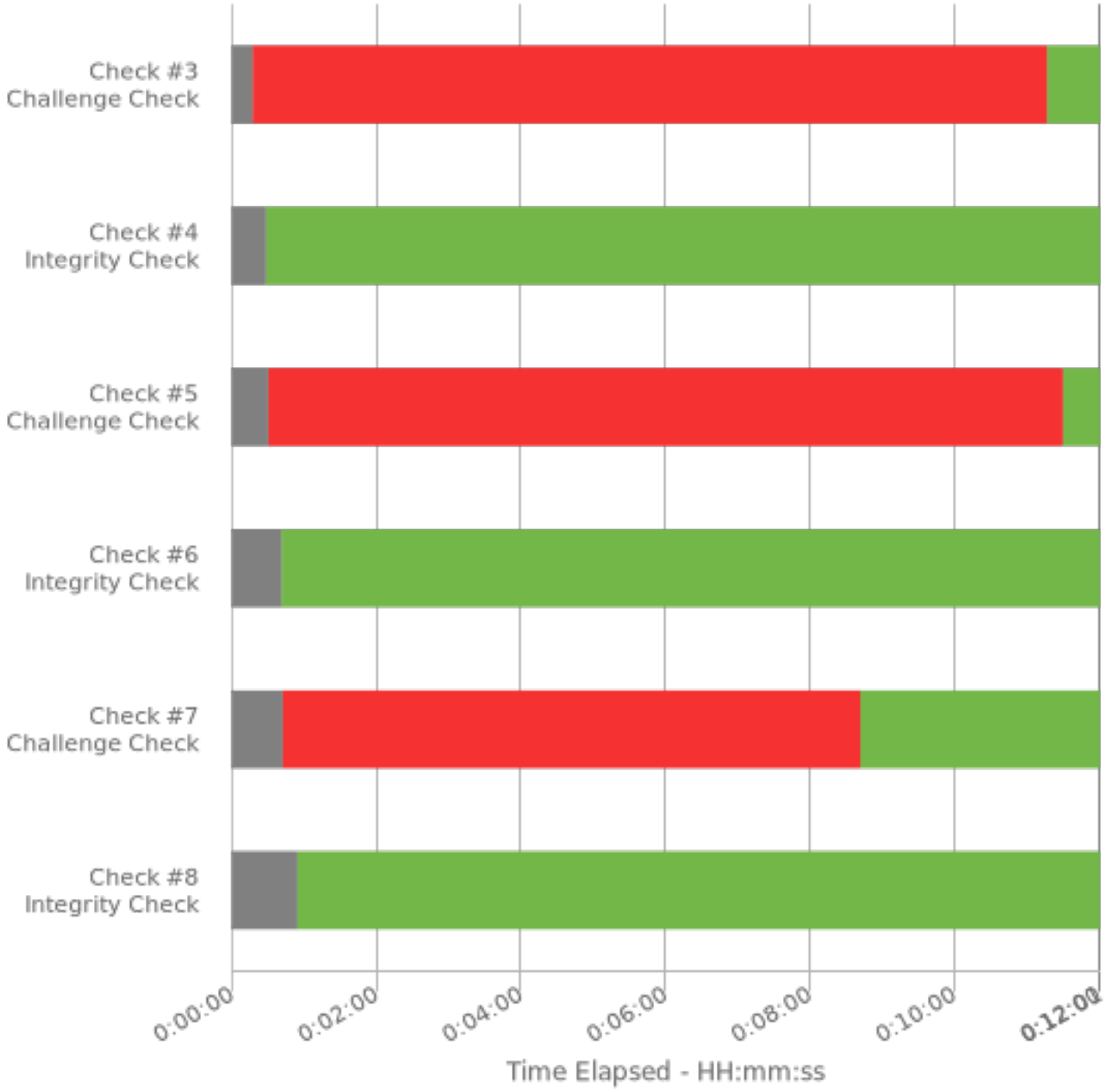
- Check #1: Remove Infected File No.1
- Check #2: Maintain File Integrity No.1 [Should be green]
- Check #3: Remove Infected File No.2
- Check #4: Maintain File Integrity No.2 [Should be green]
- Check #5: Remove Infected File No.3
- Check #6: Maintain File Integrity No.3 [Should be green]
- Check #7: Remove Infected File No.4
- Check #8: Maintain File Integrity No.4 [Should be green]

Curator Feedback

Well done!

Challenge Attempt Successful: ✔





Specialty Area

Digital Forensics

Work Role

Law Enforcement/CounterIntelligence Forensics

NICE Framework Task

T0285 Perform virus scanning on digital media.

Knowledge, Skills, and Abilities

• K0017 Knowledge of concepts and practices of processing digital forensic data.

• K0060 Knowledge of operating systems.

• K0117 Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).

• K0132 Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.

• K0133 Knowledge of types of digital forensics data and how to recognize them.

• K0187 Knowledge of file type abuse by adversaries for anomalous behavior.

• S0067 Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).

• S0073 Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).

• S0092 Skill in identifying obfuscation techniques.

Centers of Academic Excellence Knowledge Units

• Cybersecurity Foundations

• Cybersecurity Principles

• Cyber Threats

• Intrusion Detection/Prevention Systems

• Operating Systems Concepts

• Vulnerability Analysis

NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/81A03-6E6E-F8153/

Submission ID: 92945

Timestamp: 9/5/2023 3:05 AM UTC

Name: Joshua Kisner

Challenge ID: 166

Challenge Title: Preventative Protection: Thwarting the Imminent Threat [NG]

Scenario

We have received an anonymous tip that one of our systems are under imminent threat from an outside attack. Your job is to put into place proper defenses before the attack is successfully completed and our system is compromised.

Reviewed By: Solomon Zewde at Houston Community College

Duration

0:45

Full Check Pass

Full: 2/2

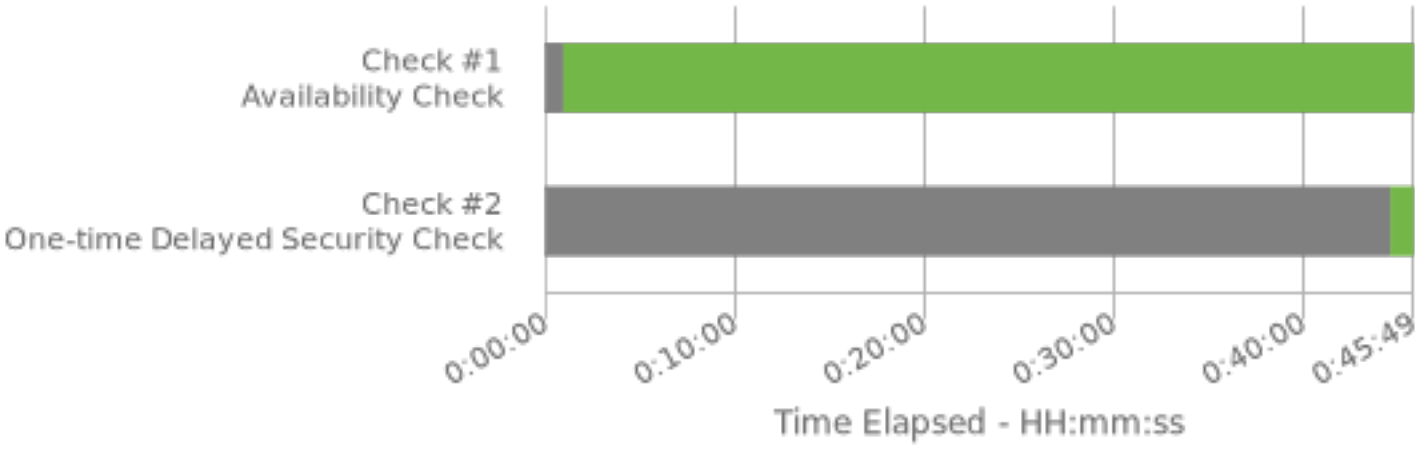
Final Check Details

- Check #1: Domain-Controller Host Check
- Check #2: Attack Thwarted

Curator Feedback

Well done!

Challenge Attempt Successful: ✔



Specialty Area

Incident Response

Work Role

Cyber Defense Incident Responder

NICE Framework Task

T0175 Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).

Knowledge, Skills, and Abilities

- K0004 Knowledge of cybersecurity and privacy principles.
- K0005 Knowledge of cyber threats and vulnerabilities.
- K0070 Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
- K0157 Knowledge of cyber defense and information security policies, procedures, and regulations.
- K0161 Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
- K0162 Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
- K0167 Knowledge of system administration, network, and operating system hardening techniques.
- S0078 Skill in recognizing and categorizing types of vulnerabilities and associated attacks.

Centers of Academic Excellence Knowledge Units

- Cybersecurity Foundations
- Cybersecurity Principles
- Cyber Threats
- Network Defense
- Operating Systems Concepts
- Vulnerability Analysis

NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/DE2A6-4534-48B7A/

Submission ID: 92949

Timestamp: 9/5/2023 3:38 AM UTC

Name: Joshua Kisner

Challenge ID: 136

Challenge Title: Security Begins & Never Ends with Updates [NG]

Scenario

We recently did a network wide security audit and found a few things that need to be addressed as soon as possible. The domain controller, production web server, and the file share servers all have either outdated software packages critical to their function or access control misconfigurations which could lead to abuse. The engineers that did the audit will fill you in on the details.

Reviewed By: Solomon Zewde at Houston Community College

Duration

0:25

Full Check Pass

Full: 3/3

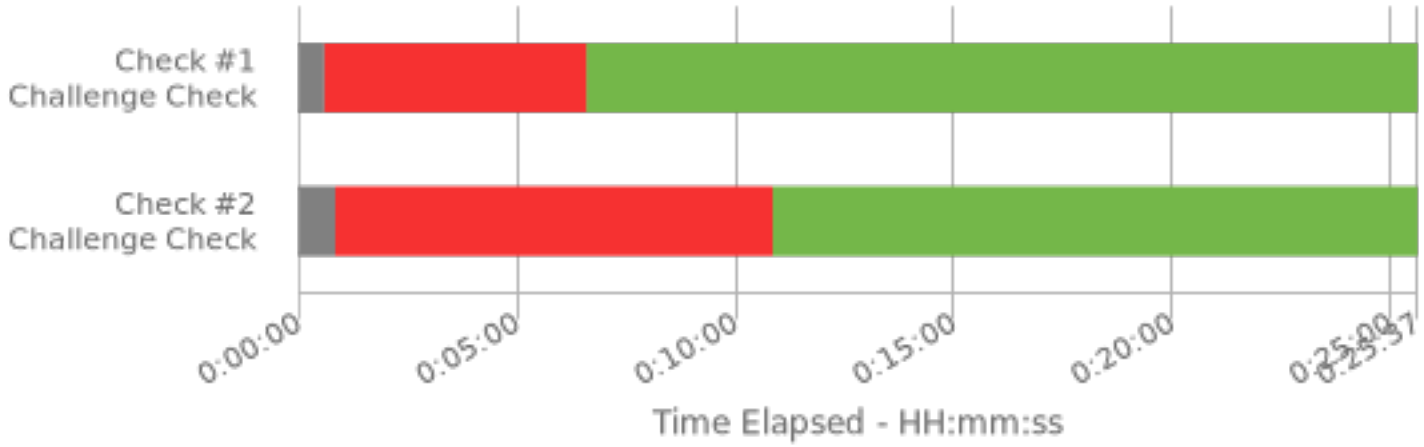
Final Check Details

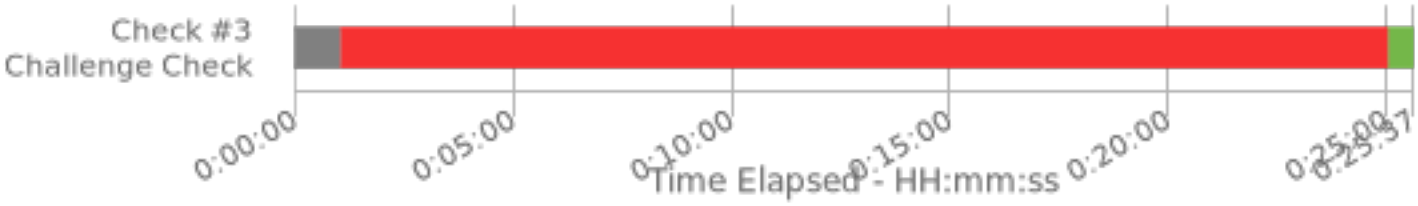
- Check #1: Guest Admin Privileges Disabled
- Check #2: Joomla Updated
- Check #3: Vulnerable FTP Updated

Curator Feedback

Well done!

Challenge Attempt Successful: ✔





Specialty Area

Network Services

Work Role

Network Operations Specialist

NICE Framework Task

T0160 Patch network vulnerabilities to ensure that information is safeguarded against outside parties.

Knowledge, Skills, and Abilities

- A0058 Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).
- K0005 Knowledge of cyber threats and vulnerabilities.
- K0038 Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
- K0049 Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
- K0071 Knowledge of remote access technology concepts.
- K0076 Knowledge of server administration and systems engineering theories, concepts, and methods.
- K0160 Knowledge of the common attack vectors on the network layer.
- K0179 Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- S0040 Skill in implementing, maintaining, and improving established network security practices.

Centers of Academic Excellence Knowledge Units

- Cybersecurity Foundations
- IT Systems Components
- Life-Cycle Security
- Network Defense
- Operating Systems Administration
- Operating Systems Concepts
- Operating Systems Hardening
- Operating Systems Theory
- Vulnerability Analysis

NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/D9CB2-3D9B-DEE02/

Submission ID: 99759

Timestamp: 11/16/2023 12:49 AM UTC

Name: Joshua Kisner

Challenge ID: 117

Challenge Title: Digital Duplicates [NG]

Scenario

Recently Gary Thatcher our senior system administrator, came across a thumb drive attached to an employee's system. According to the employee, the thumb drive was attached without their consent and they are unsure of the origin of said drive. The drive was passed to Ione Leventis one of our security analysts. Ione has attached the drive to our sheep-dip system which in our case is the Security-Desk machine. However, Ione was called away on other matters and you are now entrusted with the task. According to current company policy the thumb drive must be inspected for any malicious agents that could threaten DAS Web's overall security. Your job is to create a forensically sound duplicate image of the thumb drive using dd so it can be examined without the risk of inadvertently modifying potential evidence. SHA512 hashes should also be taken and compared between the original thumb drive which is already attached, but not mounted, to the system and the forensic image.

Reviewed By: Solomon Zewde at Houston Community College

Duration

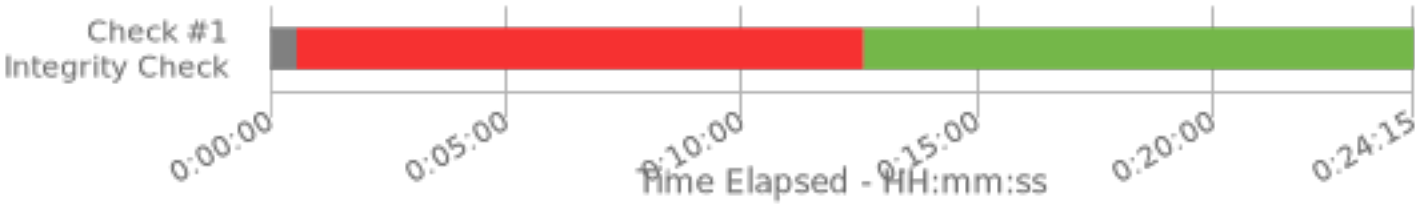
0:24

Final Check Details

Check #1: Forensic Image Created

Full Check Pass

Full: 1/1



Specialty Area

Digital Forensics

Work Role

Law Enforcement/CounterIntelligence Forensics

NICE Framework Task

T0048 Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats.

Knowledge, Skills, and Abilities

- K0017 Knowledge of concepts and practices of processing digital forensic data.
- K0021 Knowledge of data backup and recovery.
- K0042 Knowledge of incident response and handling methodologies.
- K0060 Knowledge of operating systems.
- K0117 Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).
- K0118 Knowledge of processes for seizing and preserving digital evidence.
- K0122 Knowledge of investigative implications of hardware, Operating Systems, and network technologies.
- K0132 Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.
- K0133 Knowledge of types of digital forensics data and how to recognize them.
- K0304 Knowledge of concepts and practices of processing digital forensic data.
- S0047 Skill in preserving evidence integrity according to standard operating procedures or national standards.
- S0065 Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).
- S0067 Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).
- S0073 Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).
- S0089 Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).

Centers of Academic Excellence Knowledge Units

- Cybersecurity Principles
- Digital Forensics
- IT Systems Components
- Operating Systems Concepts

NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/9014F-A42A-70164/

Submission ID: 99774

Timestamp: 11/16/2023 1:11 AM UTC

Name: Joshua Kisner

Challenge ID: 175

Challenge Title: Social Site Stoppage [NG]

Scenario

Our CEO has decided that he wants to stop employees from spending company time on social media. We need you to implement a method of blocking access to these websites.

Reviewed By: Solomon Zewde at Houston Community College

Duration

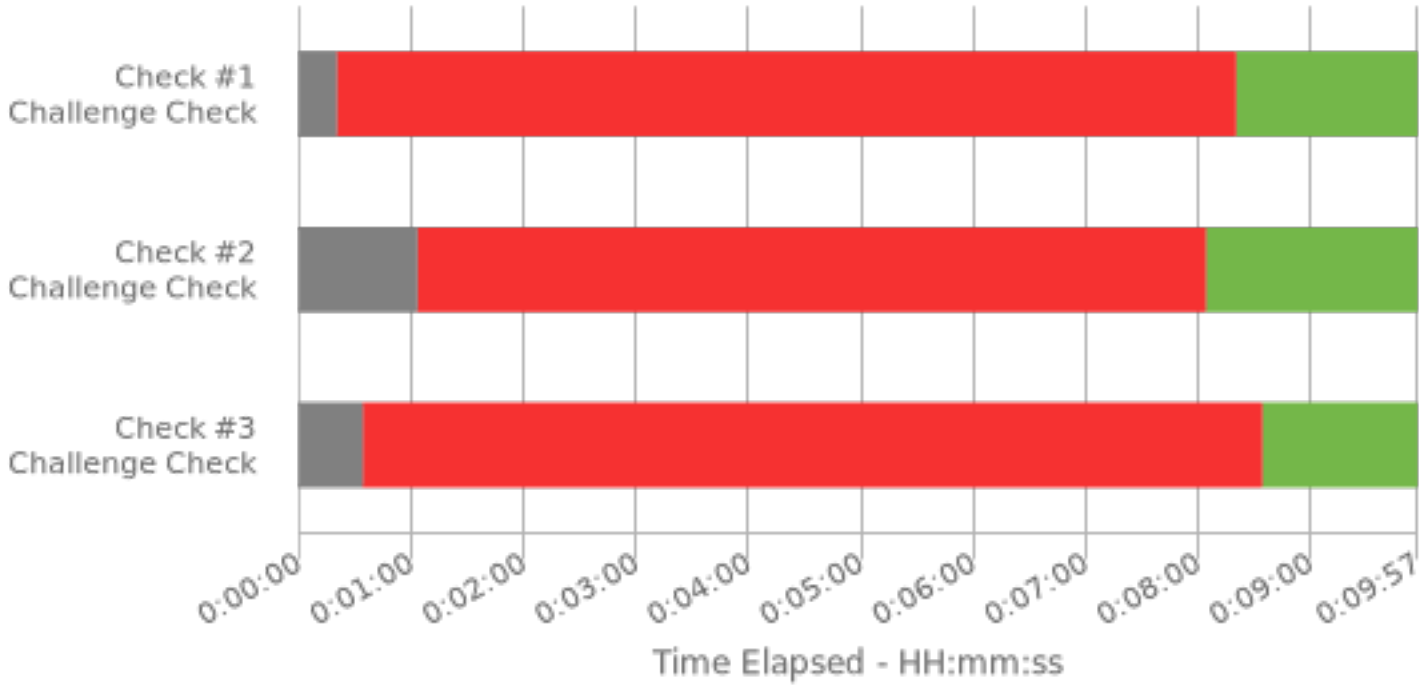
0:09

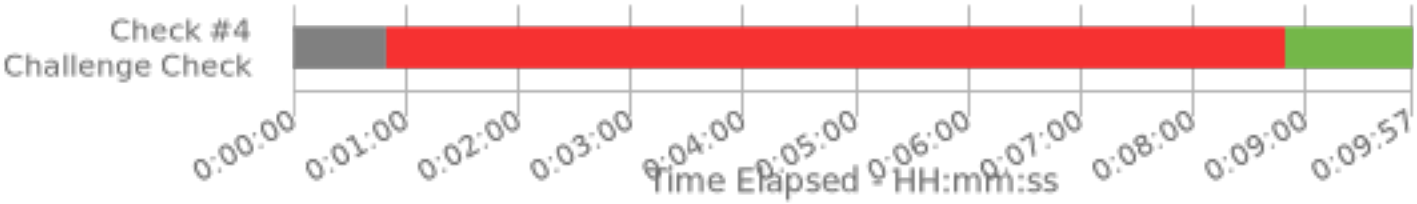
Full Check Pass

Full: 4/4

Final Check Details

- Check #1: youtube.com Being Routed to 0.0.0.0
- Check #2: twitter.com Being Routed to 0.0.0.0
- Check #3: facebook.com Being Routed to 0.0.0.0
- Check #4: instagram.com Being Routed to 0.0.0.0





Specialty Area

Network Services

Work Role

Network Operations Specialist

NICE Framework Task

T0232 Test and maintain network infrastructure including software and hardware devices.

Knowledge, Skills, and Abilities

• A0052 Ability to operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.

• A0055 Ability to operate common network tools (e.g., ping, traceroute, nslookup).

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

• K0010 Knowledge of communication methods, principles, and concepts that support the network infrastructure.

• 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]).

• K0111 Knowledge of network tools (e.g., ping, traceroute, nslookup)

• K0135 Knowledge of web filtering technologies.

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

Centers of Academic Excellence Knowledge Units

• Basic Cyber Operations

• Basic Networking

• Digital Communications

• IT Systems Components

• Network Technology and Protocols

• Operating Systems Administration