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

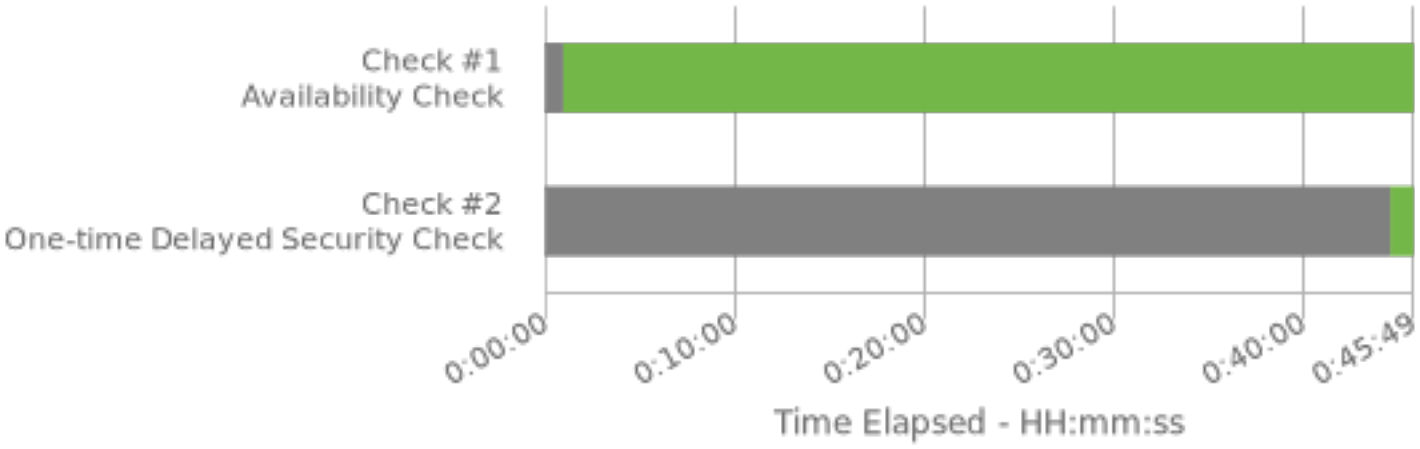
Final Check Details

- 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