NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/C2B1B-9602-34774/

Submission ID: 72511

Timestamp: 7/23/2022 11:58 AM UTC

Name: Richard Compton

Challenge ID: 71

Challenge Title: Disastrous DNS Destruction

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

Scenario

We are experiencing DNS related issues that were caused by a former employee's malicious activity. We need you to discover the root of the issue and restore access to the production website.

Duration

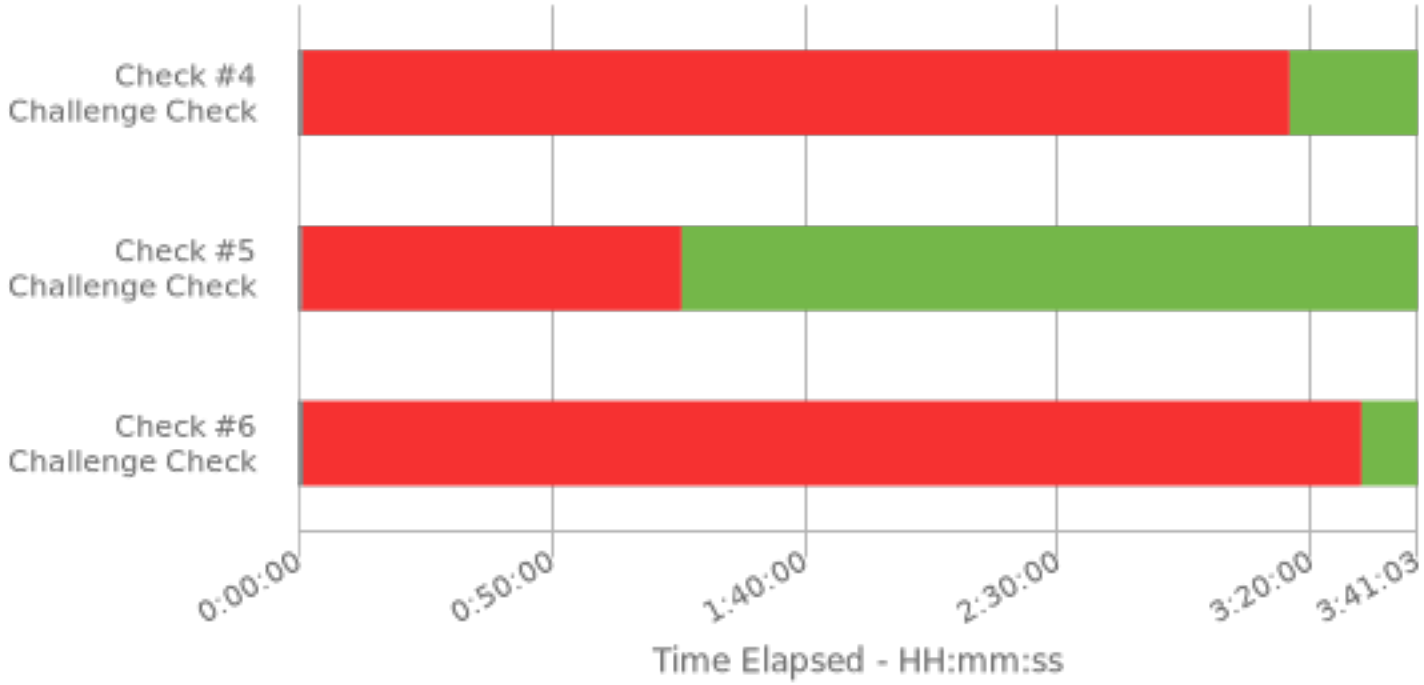
3:41

Full Check Pass

Full: 6/6

Final Check Details

- Check #1: Domain Name Resolving Problem Solved
- Check #2: DNSSEC Validation Enabled
- Check #3: Zone Signing Set
- Check #4: Pollution Protection Enabled
- Check #5: Malware Isolated on Security-Desk
- Check #6: Webroot of Malicious Website Emptied



Specialty Area

Incident Response

Work Role

Cyber Defense Incident Responder

NICE Framework Task

T0041 Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.

Knowledge, Skills, and Abilities

- K0001 Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0002 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- K0004 Knowledge of cybersecurity and privacy principles.
- K0034 Knowledge of network services and protocols interactions that provide network communications.
- K0042 Knowledge of incident response and handling methodologies.
- K0167 Knowledge of system administration, network, and operating system hardening techniques.
- K0179 Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0565 Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.
- S0077 Skill in securing network communications.

Centers of Academic Excellence Knowledge Units

- Basic Cyber Operations
- Basic Networking
- Data Administration

- Digital Communications
- IT Systems Components
- Network Technology and Protocols