NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/18439-92DB-82F85/

Submission ID: 58841

Timestamp: 11/22/2021 1:22 AM UTC

Name: Harsha Siddapura Gnaneshwara Harsha Siddapura Gnaneshwara

Challenge ID: 55

Challenge Title: Lengthy Logs: Attack Analysis

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

Scenario

Lately, employees have been having some issues logging in to one of our Wordpress websites and we can't figure out why. Our security analyst suspects that we might have been hit by a cyber attack, but is currently indisposed and can't look into it. I need you to take a look and confirm whether or not we were actually hit and if so, what the impact of that attack might have been.

Duration

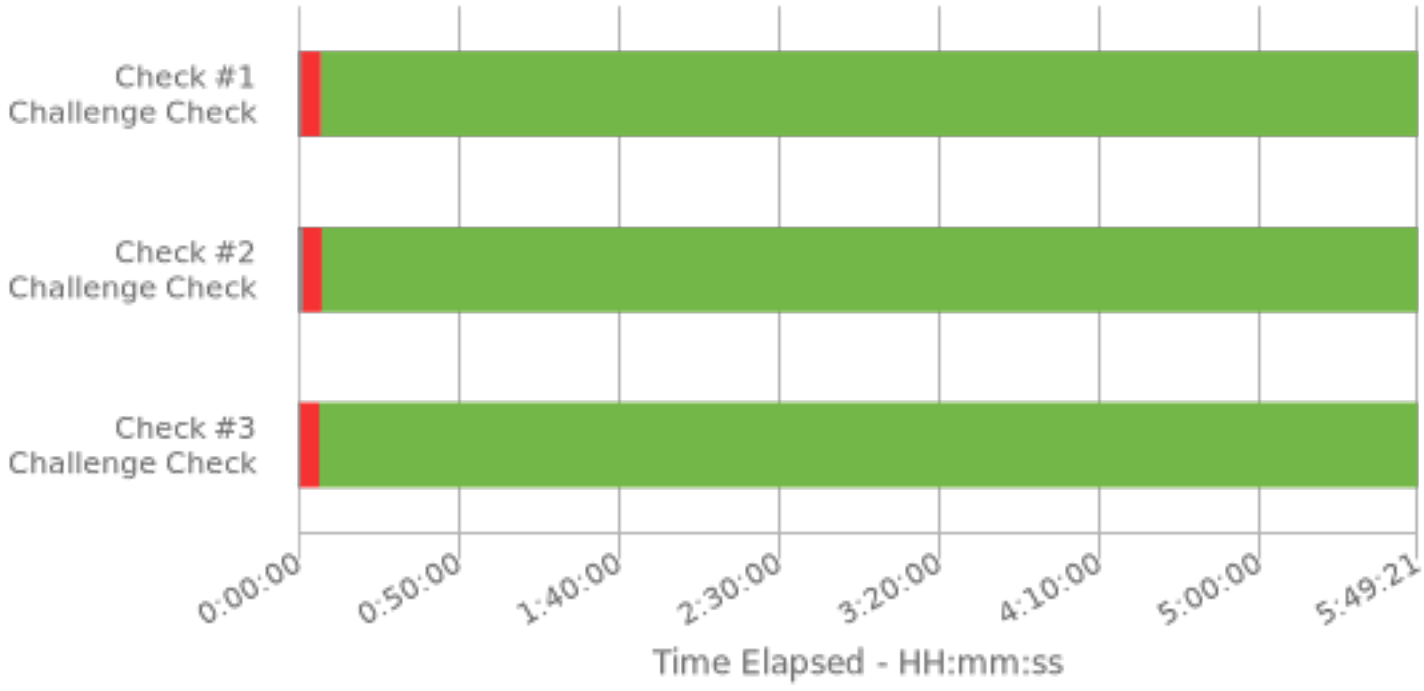
5:49

Full Check Pass

Full: 3/3

Final Check Details

- Check #1: Correctly Reported Exploited Host and Service
- Check #2: Correctly Reported Exploited Service Log File Path
- Check #3: Correctly Reported Compromised Wordpress User[s]



Specialty Area

Cybersecurity Defense Analysis

Work Role

Cyber Defense Analyst

NICE Framework Task

T0166 Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.

Knowledge, Skills, and Abilities

- K0004 Knowledge of cybersecurity and privacy principles.
- K0005 Knowledge of cyber threats and vulnerabilities.
- K0042 Knowledge of incident response and handling methodologies.
- K0044 Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- K0060 Knowledge of operating systems.
- 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).
- K0161 Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
- K0167 Knowledge of system administration, network, and operating system hardening techniques.
- K0192 Knowledge of Windows/Unix ports and services.
- K0297 Knowledge of countermeasure design for identified security risks.
- K0318 Knowledge of operating system command-line tools.

Centers of Academic Excellence Knowledge Units

- Cybersecurity Foundations
- Cybersecurity Principles
- Cyber Threats
- Operating Systems Administration
- Operating Systems Concepts
- Vulnerability Analysis