NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/3EE05-9336-C4F15/

Submission ID: 114113

Timestamp: 5/26/2024 7:50 AM UTC

Name: Colin Choquette

Challenge ID: 85

Challenge Title: Networking Anomalies: A Hunt For The Hidden

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

Scenario

You are provided a network traffic capture file that needs to be reviewed. Investigate the current state of the network, reporting any unusual or suspicious traffic.

Duration

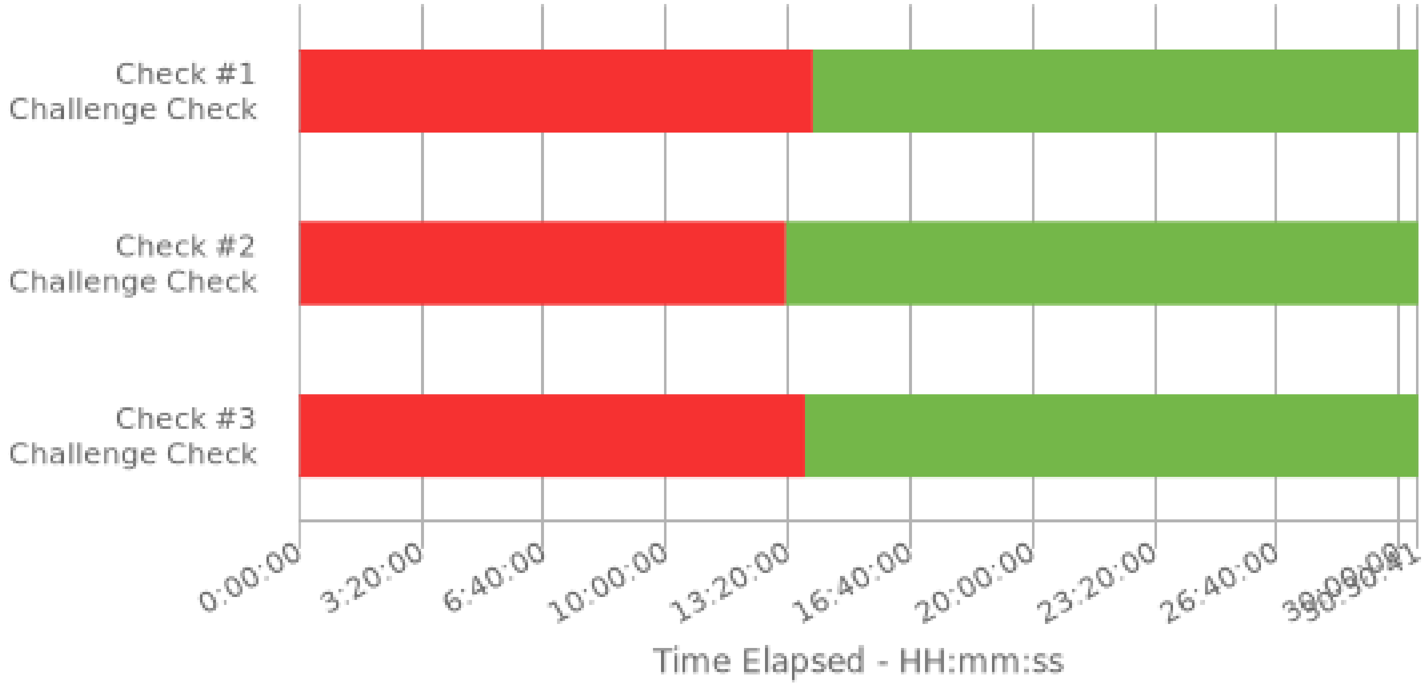
30:30

Full Check Pass

Full: 3/3

Final Check Details

- ✓ Check #1: Prod-Joomla Packet Capture Correctly Analyzed
- ✓ Check #2: Workstation Packet Capture Correctly Analyzed
- ✓ Check #3: Fileshare Packet Capture Correctly Analyzed



Specialty Area

Cybersecurity Defense Analysis

Work Role

Cyber Defense Analyst

NICE Framework Task

T0023 Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.

Knowledge, Skills, and Abilities

- K0001 Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0058 Knowledge of network traffic analysis methods.
- 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]).
- K0106 Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vulnerabilities.
- K0113 Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).
- K0301 Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
- K0332 Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- S0156 Skill in performing packet-level analysis.

Centers of Academic Excellence Knowledge Units

- Basic Networking
- Network Forensics
- Network Technology and Protocols