NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/81005-13C0-22AEC/

Submission ID: 61006

Timestamp: 1/10/2022 3:48 AM UTC

Name: Cesar Plasencia

Challenge ID: 169

Challenge Title: Networking Anomalies: The Packet Capture Edition [NG]

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

Scenario

Our security analyst has been busy with other work recently and is in need of some assistance. She needs help viewing some network traffic logs to identify if any weird activity is going on that could potentially be threats to our network resources. We need you to review a set of logs and identify malicious activity if it exists.

Duration

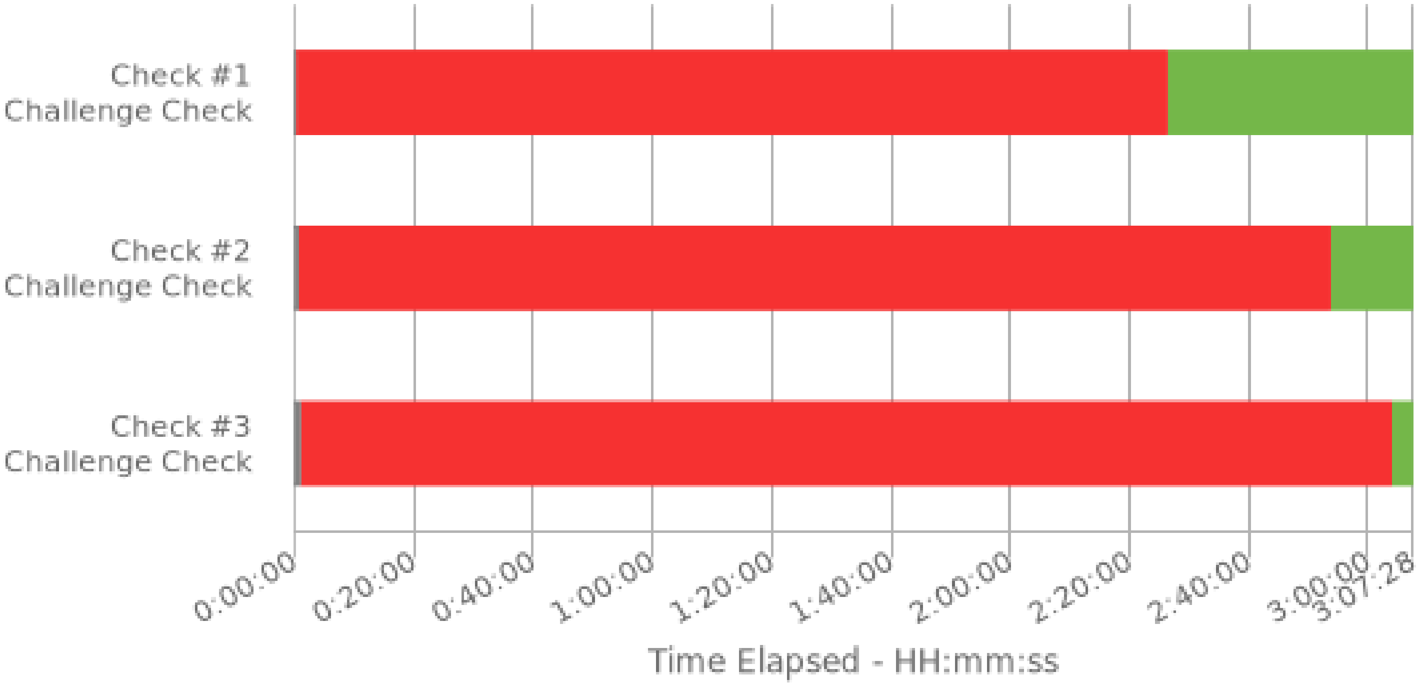
3:07

Full Check Pass

Full: 3/3

Final Check Details

- ✓ Check #1: PCAP File 10.7.pcap Analyzed Correctly
- ✓ Check #2: PCAP File 20.0.pcap Analyzed Correctly
- ✓ Check #3: PCAP File 30.21.pcap Analyzed Correctly



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.
- K0004 Knowledge of cybersecurity and privacy principles.
- K0005 Knowledge of cyber threats and vulnerabilities.
- K0033 Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
- K0042 Knowledge of incident response and handling methodologies.
- K0056 Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).
- K0058 Knowledge of network traffic analysis methods.
- K0060 Knowledge of operating systems.
- 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]).
- 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).
- 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).
- K0116 Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).
- 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.
- K0221 Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
- K0297 Knowledge of countermeasure design for identified security risks.
- K0318 Knowledge of operating system command-line tools.
- 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
- Cybersecurity Foundations
- Cybersecurity Principles
- Cyber Threats
- Network Defense

- Operating Systems Administration
- Operating Systems Concepts