NICE Challenge Project

Challenge Submission Report [BETA]

https://portal.nice-challenge.com/reports/view/ImY2YWJmY2Y1N2VjMDRkODdhYmZhOGM1MTM0MDk2NzI1Ig:1jNQpT:-CAzlCZk4Y8jKk2LiooBVgaA2zI/

Submission ID: 27020

Timestamp: 4/12/2020 12:26 AM UTC

Name: Marco Lin

Challenge ID: 60

Challenge Title: Incoming Zero Day! Prepare The IDS/IPS!

This report has not been published by a curator, therefore the NICE Challenge Project cannot support its validity.

Scenario

Our CEO hired a contractor to audit our infrastructure. The auditor discovered our webserver is vulnerable to a recently discovered exploit. Create and apply an IDS/IPS ruleset that will prevent malicious requests of this nature from reaching the web server, while leaving benign traffic uninterrupted.

Duration

0:30

Full Check Pass

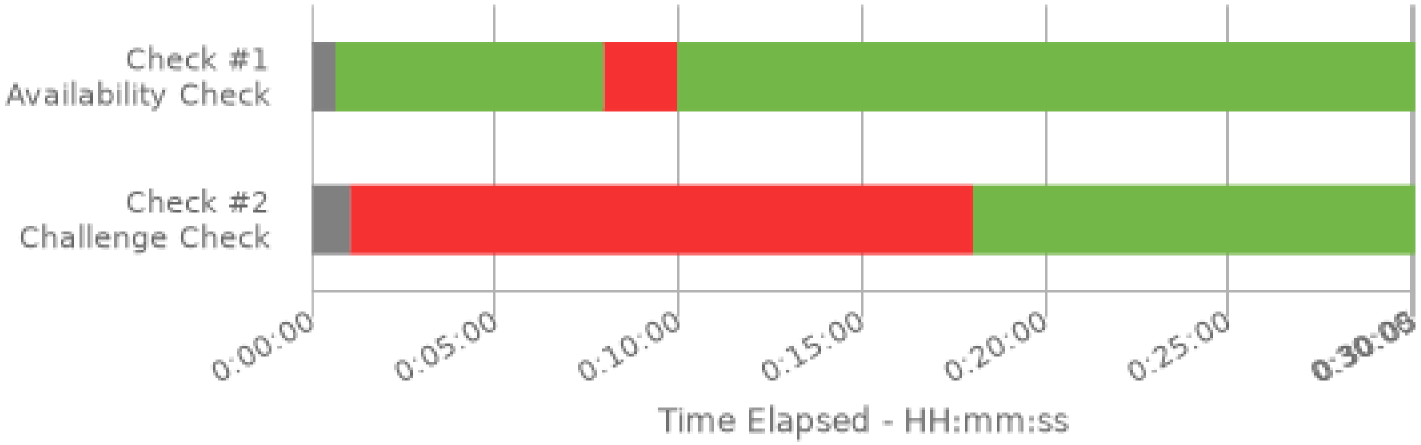
Full: 2/2

Final Check Details

- ✓ Check #1: Regular Site Traffic Undisrupted [Should Start Green]
- ✓ Check #2: Snort Logging LetMeCry Exploit Alerts

Player Documentation

Exportable challenge submissions are in beta.
Player challenge documentation is not included at this time.



Specialty Area	Work Role
Cybersecurity Defense Infrastructure Support	Cyber Defense Infrastructure Support Specialist

NICE Framework Task

T0042 Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications.

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.
- K0006 Knowledge of specific operational impacts of cybersecurity lapses.
- K0033 Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
- K0044 Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- K0062 Knowledge of packet-level analysis.
- K0106 Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
- K0157 Knowledge of cyber defense and information security policies, procedures, and regulations.
- K0160 Knowledge of the common attack vectors on the network layer.
- K0221 Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
- K0324 Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.
- K0332 Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- K0334 Knowledge of network traffic analysis (tools, methodologies, processes).
- S0007 Skill in applying host/network access controls (e.g., access control list).
- S0053 Skill in tuning sensors.
- S0077 Skill in securing network communications.
- S0079 Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
- S0121 Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).

Centers of Academic Excellence Knowledge Units

- Cybersecurity Foundations
- Cybersecurity Principles
- Cyber Threats
- Intrusion Detection/Prevention Systems
- Network Defense