NICE Challenge Project

Challenge Submission Report [BETA]

https://portal.nice-challenge.com/reports/view/IjUwNjQyY2Y5MDY4YTRiYTRiM2VkNmM3ZGYxNjE0OTJhIg:1jNQor:eQiS4CdtczPmOxo4L_3lGGmwKTM/

Submission ID: 24877

Timestamp: 3/5/2020 5:17 AM UTC

Name: Marco Lin

Challenge ID: 68

Challenge Title: Penetration Testing: Bringing Passwords Up To Snuff

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

Scenario

We have reason to believe that some of our employees have weaker than should be acceptable passwords, so we want you to conduct authorized penetration testing against various company assets to determine which employees need to change their passwords.

Duration

35:27

Full Check Pass

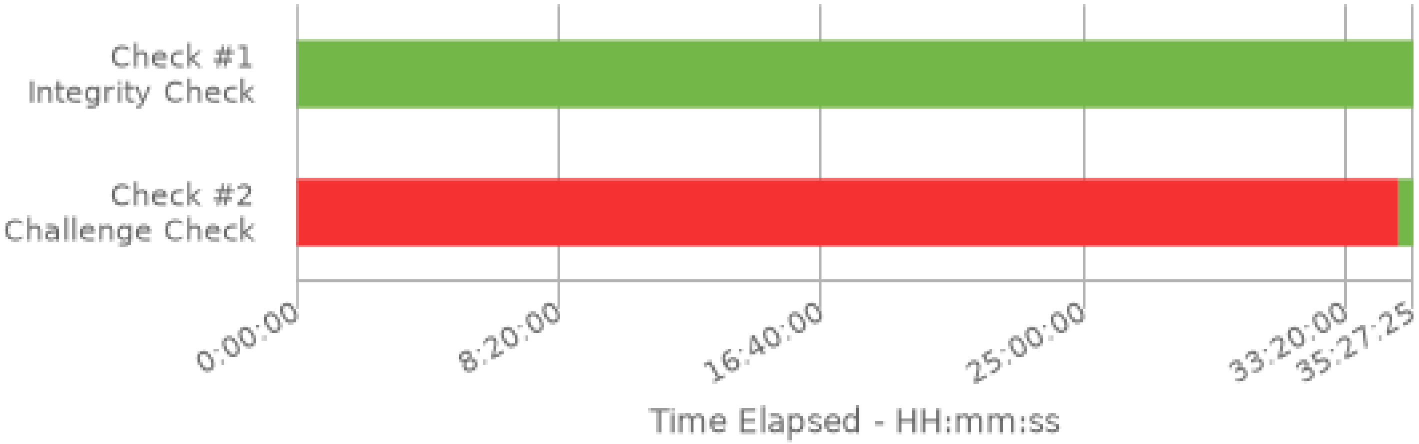
Full: 2/2

Final Check Details

- ✓ Check #1: AD Accounts That Do Not Need a Password Reset Are Not Marked for One [Should Stay Green]
- ✓ Check #2: AD Accounts That Do Need a Password Reset Are Marked for One

Player Documentation

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



Specialty Area

Vulnerability Assessment and Management

Work Role

Vulnerability Assessment Analyst

NICE Framework Task

T0028 Conduct and/or support authorized penetration testing on enterprise network assets.

Knowledge, Skills, and Abilities

- A0123 Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- K0002 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- K0003 Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- K0004 Knowledge of cybersecurity and privacy principles.
- K0005 Knowledge of cyber threats and vulnerabilities.
- K0009 Knowledge of application vulnerabilities.
- K0044 Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- K0167 Knowledge of system administration, network, and operating system hardening techniques.
- K0206 Knowledge of ethical hacking principles and techniques.
- K0342 Knowledge of penetration testing principles, tools, and techniques.
- S0044 Skill in mimicking threat behaviors.
- S0051 Skill in the use of penetration testing tools and techniques.

Centers of Academic Excellence Knowledge Units

- Cybersecurity Ethics
- Cybersecurity Foundations
- Cybersecurity Planning and Management
- Cybersecurity Principles
- Cyber Threats
- Penetration Testing
- Policy, Legal, Ethics, and Compliance
- Privacy
- Web Application Security