NICE Challenge Project

Challenge Submission Report

https://portal.nice-challenge.com/reports/verify/AFA1F-B2BB-74D71/

Submission ID: 63073

Timestamp: 2/5/2022 4:33 AM UTC

Name: Winston Lee

Challenge ID: 129

Challenge Title: Interns & HR on the Domain Controller [NG]

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

Scenario

Recently we concluded our first intern program here at DASWebs. While we expected it to be valuable to the intern, Rob, after working with our techs for a while on our network he brought to our attention that he could access critical systems with his basic domain credentials. After which we reviewed how things were setup we found that many domain users have access to servers and shares they shouldn't. The techs and I have already outlines the basic start to fixing these issues and we want you to handle it.

Duration

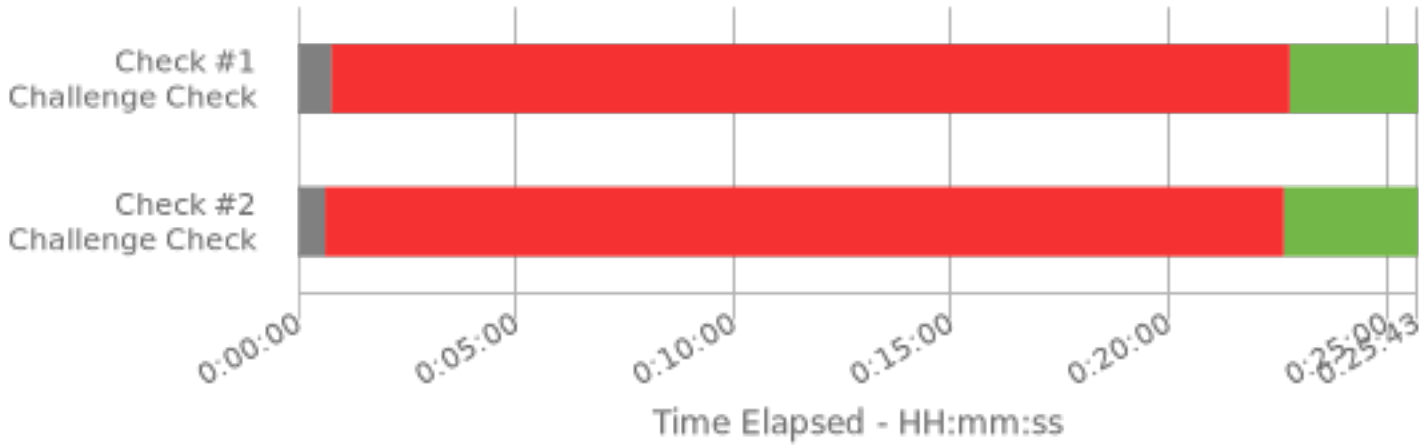
0:25

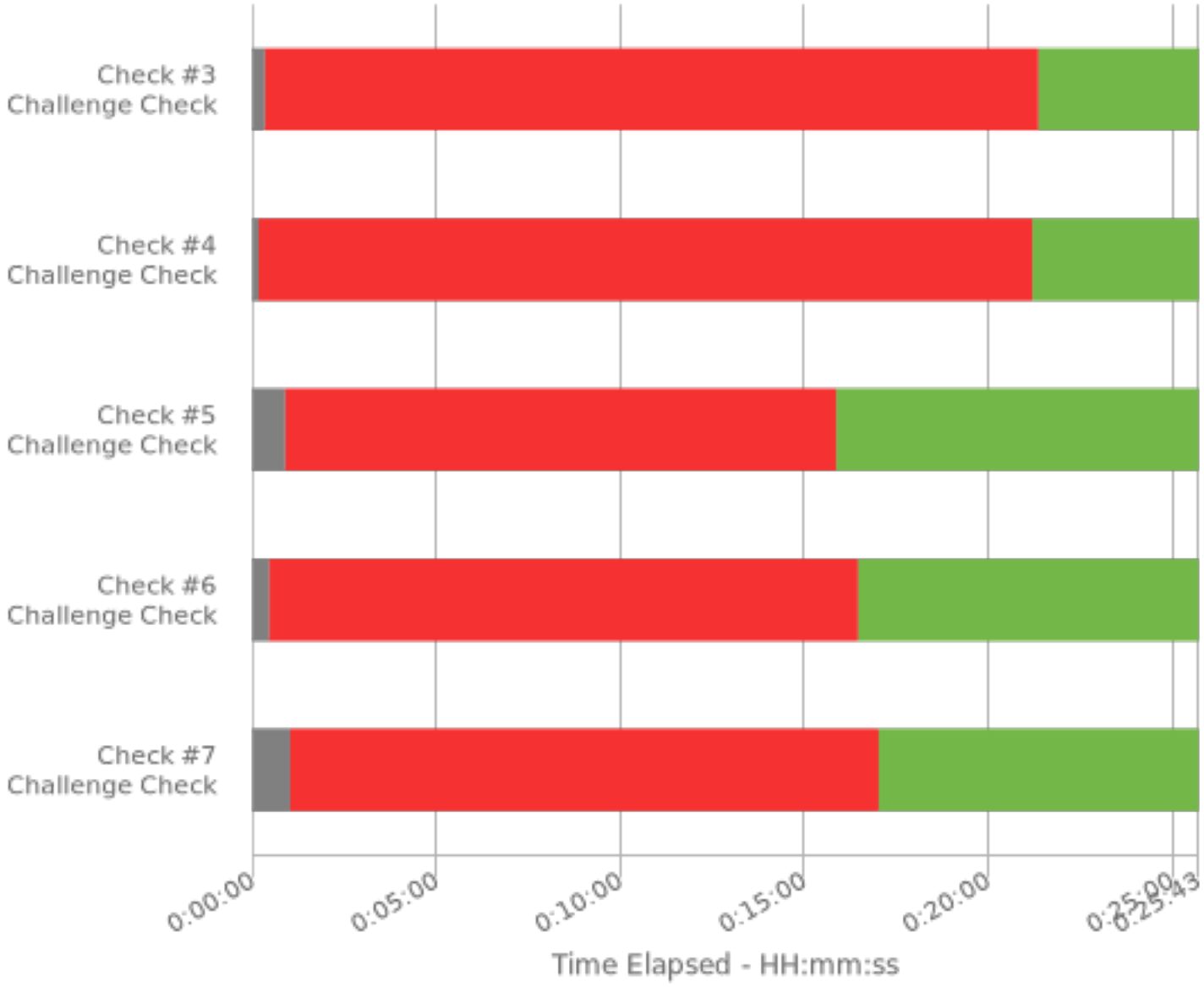
Full Check Pass

Full: 7/7

Final Check Details

- Check #1: HR Share access granted to only Sergio via HRSec security group
- Check #2: HR Share access Restricted to Domain Admins security group
- Check #3: Accounting Share access granted to only Brimlock via AccountingSec security group
- Check #4: Accounting Share access Restricted to Domain Admins security group
- Check #5: Robs Account Disabled
- Check #6: Brimlock Stones can only log onto Workstation-Desk
- Check #7: Sergio Chanel can only log onto Workstation-Desk





Specialty Area

Systems Administration

Work Role

System Administrator

NICE Framework Task

T0144 Manage accounts, network rights, and access to systems and equipment.

Knowledge, Skills, and Abilities

- K0002 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- K0004 Knowledge of cybersecurity and privacy principles.
- K0005 Knowledge of cyber threats and vulnerabilities.
- K0049 Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
- K0077 Knowledge of server and client operating systems.
- K0088 Knowledge of systems administration concepts.

• K0100 Knowledge of the enterprise information technology (IT) architecture.
• K0158 Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).
• K0167 Knowledge of system administration, network, and operating system hardening techniques.
• S0016 Skill in configuring and optimizing software.
• S0043 Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).
• S0143 Skill in conducting system/server planning, management, and maintenance.
• S0158 Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).

Centers of Academic Excellence Knowledge Units

• Cybersecurity Foundations
• Cybersecurity Principles
• Operating Systems Concepts
• Windows System Administration