Lab Report

Your Performance

Your Score: 5 of 5 (100%)

Pass Status: Pass

Elapsed Time: 2 minutes 31 seconds

Required Score: 100%

Task Summary

Required Actions

- ✓ Change the default Admin username
- ✓ Change the default Admin password
- ✓ Change the idle timeout for the Admin user to 15 minutes or less
- ✓ Limit administrative access for the Admin user to WAN only
- ✓ Limit administrative access for the Admin user to only the ITAdmin computer

Explanation

In this lab, your task is to:

- Run a vulnerability scan for the network security appliance (NSA) (198.28.56.18) using Security Evaluator on the taskbar.
- Remediate the vulnerabilities found in the vulnerability report on the NSA.
  - Rename the cisco user account using the following parameters:
    - Set a username of ***your choice***.
    - Set a password of ***your choice***.
    - Set the idle timeout to **15 minutes or less**.
    - Set LAN access only for your user (no WAN access).
    - Allow access to your user only from the ITAdmin workstation (192.168.0.31).
- Re-run a vulnerability scan to make sure all of the issues are resolved.

Complete this lab as follows:

1. Run a Security Evaluator report as follows:
   a. From the taskbar, open Security Evaluator.
   b. Next to Local Machine, select the **Target** icon to select a new target.
   c. Select **IPv4 Address**.
   d. Enter **198.28.56.18**.
   e. Click **OK**.
   f. Select the **Status Run/Rerun Security Evaluation** icon to run the security evaluation.
   g. Review the results to determine which issues you need to resolve on the NSA.
2. From the taskbar, open Chrome.
3. Maximize Chrome for easier viewing.
4. In the URL field, type **198.28.56.18** and press **Enter**.
5. In the Security Appliance Configuration utility, enter **cisco** as the username.
6. Enter **cisco** as the password.
7. Select **Log In**.
8. Rename the cisco user account as follows:
   a. From the Getting Started (Basic) page, select **Change Default Admin Password and Add Users**.
   b. Select **Edit** for the cisco username.
   c. In the User Name field, enter the ***username*** you chose.
   d. Select **Check to Edit Password**.
   e. In the Enter Current Logged in Administrator Password field, enter **cisco**.
   f. In the New Password field, enter the ***password*** you choose.
   g. In the Confirm New Password field, enter the ***password*** to confirm the new password.
   h. Enter the ***idle timeout***.
   i. Click **Apply**.

9. Edit user policies as follows:
    a. Under Edit User Policies, select **Login** to configure a login policy.
    b. Select **Deny Login from WAN Interface**.
    c. Click **Apply**.
10. Define network access as follows:
    a. Under Edit User Policies, select **By IP** to configure IP address restrictions for login.
    b. Under Defined Addresses, select **Add**.
    c. In the Source Address Type field, make sure **IP Address** is selected.
    d. In the Network Address/IP Address field, enter **192.168.0.31** for ITAdmin.
    e. Click **Apply**.
    f. Select **Allow Login only from Defined Addresses**.
    g. Click **Apply** to close the dialog.
11. Verify that all the issues were resolved using the Security Evaluator feature on the ITAdmin computer as follows:
    a. From the taskbar, open Security Evaluator.
    b. In Security Evaluator, select **Status Run/Rerun Security Evaluation** icon to rerun the security evaluation.
    c. Remediate any remaining issues.