Lab Report

Your Performance

Your Score: 0 of 5 (0%) Pass Status: Not Passed
Elapsed Time: 4 minutes 34 seconds Required Score: 100%

Task Summary

- ✗ 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 LAN only
- ✗ Limit administrative access for the Admin user to only the ITAdmin computer

Explanation

In this lab, you perform the following:

- Rename the cisco user account according to the following parameters:
  - Username: ***your choice***
  - Password: ***your choice***
  - Idle timeout: **15 minutes or less**
  - Set for LAN access only (no WAN access) for your user.
  - Allow access to your user only from the ITAdmin workstation (**192.168.0.31**).

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 the ***IP address*** of the Network Security Appliance.
   e. Click **OK**.
   f. Select the **Status refresh 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 **Internet Explorer**.
3. Maximize **Internet Explorer**.
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. Click **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 enter, enter **cisco**.
   f. In the New Password field, enter the ***password*** you choose.
   g. Re-enter the new ***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. Select **Add**.
    c. In the Source Address Type field, make sure **IP Address** is selected.
    d. In the Network Address/IP Address field, enter the ***IP address*** for ITAdmin.
    e. Click **Apply**.
    f. Select **Allow Login only from Defined Addresses**.
    g. Click **Apply** to close the dialog.
11. Re-run the security evaluator to confirm the remediation of reported vulnerabilities.