**Test Specification**

**Group 15**

April 26th, 2020

**Team Members**

Domonic Neal

Ny Tran

Ronny Soto

|  |  |
| --- | --- |
| **Test Case ID:** | 4.1.1.1 |
| **Title:** | Authenticating A User To A Guest Network |
| **Feature/Subfeature:** | System User Validation |
| **Purpose:** | To confirm that a user is able to log-in to and access the Guest Network applications or data on |
| **Initial Conditions:** | A User must have a device that should be able to connect to a network |
| **Test Data:** | Test Data will include invalid usernames such as usernames starting with symbols ‘!@#$#%^&\*’ and invalid passwords as in ‘1234’ and ‘cooldog’. Valid usernames and passwords will also be used, but will not be listed here for security and confidentiality reasons. |
| **Test Actions:** | 1. Open wireless settings on device 2. Click on ‘Guest Network’ 3. Click on ‘Connect’ 4. Open on the browser 5. Enter valid username and password into log-in page 6. Select ‘Ok’ |
| **Expected Results:** | After step 3, a pop-up box with a log-in prompt will appear and ask the user to input their username and password. After step 5, if the user entered a valid username and password, the device will successfully connect to the internet |

|  |  |
| --- | --- |
| **Test Case ID:** | 4.1.1.2 |
| **Title:** | Authenticating A User To The Company Network |
| **Feature/Subfeature:** | System User Validation |
| **Purpose:** | To confirm that only employees of the company are able to log in and have access to our applications |
| **Initial Conditions:** | Users must have a company issued device that can connect to the internet with their unique log-in. |
| **Test Data:** | Test Data will include invalid usernames such as usernames starting with symbols ‘!@#$#%^&\*’ and invalid passwords as in ‘1234’ and ‘cooldog’. Valid usernames and passwords will also be used, but will not be listed here for security and confidentiality reasons. |
| **Test Actions:** | 1. Open wireless settings on device 2. Click on ‘Company Network’ 3. Click on ‘Connect’ 4. Enter valid username and password into log-in page 5. Select ‘Ok’ 6. Open browser and accept Terms of Use and Disclaimer |
| **Expected Results:** | After step 3, a pop-up box with a log-in prompt will appear based on what Operating System is being used. After step 5, if the user entered a valid username and password, the user will be authenticated to the company network. In Step 6, on the browser a pop-up will appear asking the user to accept the terms of use and disclaimer |

|  |  |
| --- | --- |
| **Test Case ID:** | 4.1.2.1 |
| **Title:** | Create a User in AWS managed Active Directory |
| **Feature/Subfeature:** | System User Creation |
| **Purpose:** | Ensure that users can be created for the networks |
| **Initial Conditions:** | Employees must have an account ready, admin access, and authenticated |
| **Test Data:** | Sample user data (first name, last name, username, password, location, role, phone number) |
| **Test Actions:** | 1. Open Administrative Tools 2. Click ‘Users and Computers section’ 3. Click on a desired domain 4. Right click ‘Users’ 5. Click ‘New User’ 6. Enter sample user data, not including the password 7. Type in password and confirm that it is matching 8. Click ‘Finish’ |
| **Expected Results:** | After step 3, administrators should be taken to the section showing current users and add a user button. After step 5, a pop-up window with input fields will appear. After step 8, the user should be created and added to the desired domain. |

|  |  |
| --- | --- |
| **Test Case ID:** | 4.1.2.2 |
| **Title:** | Devices are able to see one another on the Network |
| **Feature/Subfeature:** | Device Communication |
| **Purpose:** | To confirm that devices are able to communicate with one another using the network |
| **Initial Conditions:** | Devices are connected via Wi-Fi or ethernet cable |
| **Test Data:** | ICMP packets (~50 bytes) |
| **Test Actions:** | 1. The device is connected to the internet 2. Open up command prompt 3. Send the ping command from host device to the target device |
| **Expected Results:** | After step 3, if the device is correctly configured and is visible on the network, the host device will receive a reply when the target device is pinged. If the device is not discoverable, no data will be received and the reply will state that the host is unreachable. |