11 - Blocking Threats with User-ID

1.2 Examine Firewall Configuration

In this section, you will review the settings that another administrator has configured for Application
Groups and Security policy rules.

1. Select Policies > Security. Click the Allow-All-Acquisition policy.
2. In the Security Policy Rule, select the Source tab. Note that the Source Zone is set to Acquisition.
3. Select the Destination tab. Note that the Destination Zone is set to any.
4. Select the Application tab. Note that the Application is set to Any.
5. Select the Actions tab. Note that the Action is set to Allow. Click OK.
6. Clear the counters for all Security policy rules by clicking Reset Rule Hit Counter > All rules at the bottom of the window.
7. In the Reset window, click Yes.
8. Select Objects > Application Groups and note the two new Application Groups.
9. Minimize the Palo Alto Networks Firewall open and continue to the next task.

1.3 Generate Traffic from the Acquisition Zone

In this section, you will configure a packet capture on the firewall's data plane. The goal of the packet capture is to identify a unique bit pattern that can be used to create a custom application signature.

1. On the client desktop, open the Remmina application.
2. Double-click the entry for Server-Extranet.
3. In the CLI connection, enter the following command.

   ```
   paloalto42@extranet1:~$ cd /home/paloalto42/pcaps92019/app.pcaps
   <Enter>
   ```

4. In the CLI connection, enter the following command.
   `paloalto42@extranet1:~/pcaps92019/app.pcaps$ ./Appgenerator-2.sh <Enter>`
5. Verify the Appgenerator-2 script is running.
6. Reopen the PA-VM firewall web interface by clicking on the Chromium icon in the taskbar.
7. Select Monitor > Logs > Traffic. Clear any filters in place. Note that almost all traffic is hitting the Allow-All-Acquisition Rule. Please allow the firewall 3 to 6 minutes for the traffic logs to update.
8. Add the Source User column, if necessary, to the table by clicking the small triangle in any header
   and choosing Columns > Source User.

Some columns have been hidden to show what is presented in the above screen shot. You may hide and show columns as needed for the duration of this lab.

9. Drag and drop the Source User column between the Receive Time and Source columns.
10. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.4 Enable User-ID on the Acquisition Zone

In this section, you will enable User-ID on the Acquisition security zone as part of the process of
enabling User-ID on a firewall.

1. Select Network > Zones. Click Acquisition to open the zone.

This action will make it easier for you to locate Source User information later in this lab.

2. In the Zone window, select the Enable User Identification check box. Click OK.
3. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.5 Modify the Allow-All-Acquisition Zone

In this section, you will now change the set of applications that Acquisition users are allowed to access
by modifying the existing Allow-All-Acquisition rule.

1. Select Policies > Security. Click Allow-All-Acquisition.
2. In the Security Policy Rule window, under the General tab, change the name of this rule to Allow□Corp-Apps. For Description, type Allows only approved apps for Acquisition users.
3. Select the Application tab, uncheck the option for Any. Click Add and enter the first few letters of the Allowed-Corp-Apps to display the Application Groups available. Click OK.
4. Leave the Palo Alto Networks Firewall open and continue to the next task.
5. Select Policies > Security. Click Add.
6. In the Security Policy Rule window, under the General tab, enter Allow-Mktg-Apps for the Name. For Description, enter Allows only users of marketing group to access Mktg apps.
7. Select the Source tab, under Source Zone, click Add. Select Acquisition. Under the Source User column, click Add and enter marketing.
8. Select the Destination tab. Use the dropdown list at the top to select any in the Destination Zone.
9. Select the Application tab and uncheck the option for Any. Click Add and enter the first few letters of the Allowed-Mktg-Apps to display the Application Groups available. Select Allowed-Mktg-Apps. On the right

side of the Application window, place a check in the checkbox beside DEPENDS ON. Click Add to Current Rule.

10. Notice the Applications have now been added to the Applications window.
11. Select the Actions tab and verify the Action is set to Allow. Click OK.
12. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.7 Create Deny Rule

In this section, you will create a security policy rule that allows hosts in the Users_Net to access the Custom Application in the Extranet zone.

1. Select Policies > Security. Click Add.

When you create a new Security policy rule, the default setting for Action is Allow. However, it is always a good practice to verify this setting before closing the window.

2. In the Security Policy Rule window, under the General tab, enter Deny-All-Others for the Name.
    - For Description, enter Denies non-approved applications for users in Acquisition zone.
3. Select the tab for Source, click Add, and select Acquisition.
4. Select the tab for Destination, use the dropdown list at the top to select any.

Note that you do not need to specify any users or user groups under the Source User column. Because the dropdown list is set to any, this rule will deny traffic to any user, regardless of group membership.

5. Select the tab for Application and verify that Any is checked.
6. Select the Actions tab and change the Action Setting to Deny. Click OK.

7. Verify that the Deny-All-Others rule appears at the bottom of the security policy.
8. Click the Commit link located at the top-right of the web interface.
    - If the “Deny-All-Others” rule does not appear at the bottom of the ruleset, use the Move Down button to place the rule just above the “intrazone-default” rule.
9. In the Commit window, click Commit to proceed with committing the changes.
10. When the Commit operation successfully completes, click Close to continue.
11. Minimize the Palo Alto Networks Firewall and continue to the next task.

1.8 Generate Traffic from the Acquisition Zone

1. Open the Remmina application by clicking on the Server-Extranet tab in the taskbar if necessary.
2. Ensure you are still in the app.pcaps directory. In the CLI connection, enter the following command.
    - `paloalto42@extranet1:~/pcaps92019/app.pcaps$ ./Appgenerator-2.sh`
3. Verify the Appgenerator-2 script is running.
4. Close the Server-Extranet connection by clicking the X icon.
5. Reopen the PA-VM firewall web interface by clicking on the Chromium icon in the taskbar.
6. Leave the Palo Alto Networks Firewall open and continue to the next task.

Allow the Appgenerator-2 script to complete before continuing to the next task.

1.9 Exam User-ID Logs

You can see information about User-ID through the firewall CLI or in the web interface. In this section, you will use both tools to examine User-ID entries.

1. Select Monitor > Logs > User-ID. The firewall should have numerous entries with username-to-ip□address mappings. If the User mappings are not showing, repeat Task 11.8.
2. Minimize the PA-VM firewall by clicking minimize in the upper-right of the web interface and continue to the next task.
3. On the client desktop, in the taskbar, reopen the Remmina application.
4. Double-click the entry for Firewall-A.
5. If you get Connecting to 'Firewall-A'… window, click OK.
6. In the firewall CLI, enter the following command to display entries for User-ID. Examine the User-ID information.
    - `admin@firewall-a> show user ip-user-mapping all <Enter>`
7. Close the Firewall-A window by clicking the close icon.
8. Reopen the PA-VM firewall web interface by clicking on the Chromium icon in the taskbar and continue to the next task.

The Firewall-A connection in Remmina has been pre-configured to provide login credentials to the firewall so that you do not have to log in each time. This is for convenience in the lab only.

1.10 Examine Firewall Traffic Log

Create and apply filters to view rules and users.

1. `Select Monitor > Logs > Traffic`. In the filter builder, type `( app eq youtube-base )`. Click Apply Filter.
2. Clear the filter, and in the filter builder, type `( app eq dns )`. Click Apply Filter.
3. Clear the filter, and in the filter builder, type `( app eq facebook-base )`.Click Apply Filter.

4. In the filter builder, type `( app eq facebook-base ) and (action eq allow )`. Click Apply Filter.
5. Clear the filter and in the filter builder, type `( app eq instagram-base ) and ( user.src eq ‘chicago\bbart’ )`. Click Apply Filter.
6. The lab is now complete; you may end your reservation.