15 - Implementing Day - One Best Practice Configuration

1.1 Apply a Baseline Configuration to the Firewall
In this section, you will load the firewall configuration file.

1. Log in to the firewall web interface as username admin, password Pal0Alt0!.
2. In the web interface, navigate to Device > Setup > Operations and click on Load named configuration snapshot underneath the Configuration Management section.
3. In the Load Named Configuration window, select edu-210-lab-15.xml from the Name dropdown box and click OK.
4. In the Loading Configuration window, a message will show Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed. Click Close to continue.
5. Click the Tasks icon located at the bottom-right of the web interface.
6. In the Task Manager – All Tasks window, verify the Load type has successfully completed. Click Close.
7. Click the Commit link located at the top-right of the web interface.
8. In the Commit window, click Commit to proceed with committing the changes.
9. When the Commit operation successfully completes, click Close to continue.
10. Minimize the Palo Alto Networks Firewall and continue to the next task.

1.2 Generate Traffic Without Security Profiles
In this section, you will create a new security policy rule and attempt to leave out the description. This

will let you see what happens when an administrator does not provide adequate information when
creating a rule.

1. On the client desktop, open the Remmina application.

The commit process takes changes made to the firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

2. Double-click the entry for Server-Extranet.
3. In the CLI connection, enter the following command to change the working directory.
    - `paloalto42@extranet1:~$ cd pcaps92019/attack.pcaps/ <Enter>`
4. In the CLI connection, enter the following command to run the simulated attacks.
    - `paloalto42@extranet1:~/pcaps92019/attack.pcaps$ ./malwareattacks.sh <Enter>`
5. Minimize the Remmina connection window.

This action will open an SSH connection to the server and automatically log you in with appropriate credentials.
This script takes about 6 minutes to complete. Allow the malwareattacks script to run uninterrupted.

6. On the client desktop, open the Firefox Web Browser application.
7. Type http://192.168.50.80/badtarfile.tar and press Enter.
8. In the Opening badtarfile.tar window, select Save File. Click OK.
9. In the Firefox Web Browser, open a new tab. Type http://192.168.50.80/companyssns.txt and press Enter. The browser will display a file with fictitious names and social security numbers.
10. Close the Firefox browser.
11. On the client desktop, open Terminal Emulator.

12. Enter the following command to generate a DNS query using dig to resolve a URL to an IP address.

The command returns a public IP address, indicating that the URL is accessible.
C:\home\lab-user\Desktop\Lab-Files> dig @8.8.8.8 www.quora.com

13. Leave the Terminal Emulator window open because you will use it again later in this lab.
14. Reopen the PA-VM firewall by clicking on the Chromium icon in the taskbar.
15. Leave the Palo Alto Networks Firewall open and continue to the next task.

Quora.com is one of the entries included in the malicious domains external dynamic list you configured in an earlier lab.
Also note that you may see a different IP address than what the screen shot shows.

1.3 Modify Existing Security Policies
In previous labs, you created Security Profiles to inspect traffic for spyware and virus signatures. You created a Security Profile for WildFire that forwards unknown executable files to the WildFire cloud for inspection. And you created a URL Filtering Profile to prevent users from browsing to potentially harmful categories of websites. In this section, you will review these profiles.

1. Select Objects > Security Profiles > Antivirus. Click Corp-AV.
2. In the Antivirus Profile window, for Description, enter Standard antivirus profile for all security policy rules. Check the box for Enable Packet Capture.
3. Click OK to close the Antivirus Profile window.
4. Select Objects > Security Profiles > Anti-Spyware. Click outbound-as.

Enabling Packet Capture instructs the firewall to take very small packet captures (more like packet snippets) that contains patterns in traffic which match the signatures used in the profile.

5. In the Anti-Spyware Profile window, change the Name to Corp-AS. Select the tab for DNS Policies.
6. On the DNS Policies tab, for the malicious-domains-edl entry, change the Policy Action to sinkhole. Change the Packet Capture to single-packet. Click OK.
7. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.4 Create A Corporate Vulnerability Security Profile

In this section, you will create a vulnerability Security Profile. Palo Alto Networks provides two vulnerability profiles which you can use as the basis for your own – strict and default.

1. Select Objects > Security Profiles > Vulnerability Protection. Place a check in the box beside strict. Click Clone.
2. In the Clone window, click OK.
3. Click the entry for strict-1 to open it.
4. In the Vulnerability Protection Profile window, change the Name to Corp-Vuln. For Description, enter Standard vulnerability profile for all security policy rules. Click OK.
5. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.5 Create A Corporate File Blocking Profile

In this section, you will configure a File Blocking Security Profile that the firewall will use to help detect, report, and block attempts to download potentially harmful filetypes. Palo Alto Networks provides two file blocking profiles that you can use as the basis for your own – basic file blocking and strict file blocking.

You will clone the strict file blocking profile and modify it to function as your Corp-FileBlock profile.

1. Select Objects > Security Profiles > File Blocking. Place a check beside the entry for strict file blocking. Click Clone.
2. In the Clone window, click OK.
3. Click the entry for strict file blocking-1 to open it.
4. Change the Name to Corp-FileBlock. For Description, enter Standard file blocking profile for all security policy rules. Click OK.
5. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.6 Create Data Filtering Profiles

1. Select Objects > Custom Objects > Data Patterns. Click Add.
2. In the Data Patterns window, for Name, enter US-SSNs. For Description, enter US Social Security Numbers. Change the Pattern Type to Predefined Pattern.
3. Click Add and scroll down the available list and select Social Security Numbers. Click Add again and select Social Security Numbers (without dash separator). Click OK.
4. Select Objects > Security Profiles > Data Filtering. Click Add.
5. In the Data Filtering Profiles window, for Name, enter Corp-DataFilter. For Description, enter Standard data filtering profile for all security rules.
6. Click Add and select the US-SSNs data pattern that you defined. Click in the Alert Threshold field and change the value to 1. Click in the Block Threshold field and change the value to 3. Change the Log Severity to critical. Click OK.
7. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.7 Create a Security Profile Group

To simplify the process of applying Security Profiles to Security policy rules, you can create a Security Profile Group which contains individual Security Profiles. You can then apply the Security Profile Group to a Security policy rule, rather than individually selecting each profile for each rule. In this section, you will create a Security Profile Group called Corp-Profiles-Group. You will add each of your Corp-* Security Profiles to the group.

1. Select Objects > Security Profile Groups. Click Add.
2. In the Security Profile Group window, enter Corp-Profiles-Group for the Name. For each of the available Profiles, use the dropdown list to select the Corp-* entry you have created. Click OK.
3. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.8 Apply the Corp-Profiles-Group to a Security Policy

In this section, you will apply the Corp-Profiles-Group to a security policy. With the Security Profiles in place, you can modify your security policy rules to use these protections.

1. Select Policies > Security.
2. Individually edit each security policy rule which allows traffic and change the Profile Setting under the Action tab to use the Corp-Profiles-Group. Be sure to edit and modify each of these rules.
    - Users_to_Extranet – Click OK.
    - Users_to_Internet – Click OK
    - Extranet_to_Internet – Click OK
    - Extranet_to_Users_Net – Click OK
    - Allow-PANW-Apps – Click OK
    - Acquisition-Allow-All – Click OK
3. Verify each of the rules you modified is showing the Corp-Profiles-Group by hovering over the Profile icon for each rule.

4. Click the Commit link located at the top-right of the web interface.
5. In the Commit window, click Commit to proceed with committing the changes.
6. When the Commit operation successfully completes, click Close to continue.
7. Minimize the Palo Alto Networks Firewall and continue to the next task.

1.9 Generate Attack Traffic with Security Profiles

In this section, you will generate attack traffic with security policies.

1. Reopen the Remmina application by clicking the icon in the taskbar.
2. In the CLI connection, enter the following command to change the working directory. If you are already in the attack.pcaps directory, please proceed to the next step.
    - `paloalto42@extranet1:~$ cd pcaps92019/attack.pcap/ <Enter>`
3. In the CLI connection, enter the following command to run the simulated attacks.
    - `paloalto42@extranet1:~/pcaps92019/attack.pcaps$ ./malwareattacks.sh <Enter>`
4. Minimize the Remmina connection window.
5. On the client desktop, open the Firefox Web Browser application.
6. Type http://192.168.50.80/badtarfile.tar and press Enter.
7. You should receive a File Transfer Blocked page from the firewall.
    - This script takes about 6 minutes to complete. Allow the malwareattacks script to run uninterrupted.
8. In Firefox, open a new tab. Type http://192.168.50.80/companyssns.txt and press Enter.
9. You should receive a Data Transfer Blocked page from the firewall.
10. Close the Firefox Web Browser by clicking the close icon.
11. On the client workstation, locate the open Terminal Emulator window you used earlier in this lab.

- You can maximize by clicking the Terminal icon in the taskbar.
  This page indicates that the firewall has blocked the transfer using the Data Filtering Profile and Data Pattern you defined for Social Security Numbers.

12. Enter the following command to generate a DNS query using dig to resolve a URL to an IP address.

The command returns a public IP address, indicating that the URL is accessible. It will now show the www.quora.com DNS query is now in the sinkhole.paloaltonetworks.com. C:\home\lab-user\Desktop\Lab-Files> dig @8.8.8.8 www.quora.com

13. Reopen the PA-VM firewall by clicking on the Chromium icon in the taskbar.

This indicates that the firewall has intercepted and sinkholed the DNS query using the DNS Sinkholing function in your Anti-Spyware profile.

14. In the firewall web interface, select Monitor > Logs > Threat. Clear any filters in place and press Enter. The Threat Log should contain numerous entries for Spyware and Vulnerabilities.
15. Select Monitor > Logs > URL Filtering. Note the numerous entries for blocked URLs.

These entries indicate that the firewall has blocked malicious traffic using the Vulnerability and Anti-Spyware profiles that you defined. Note that the entries you see in the Threat Log may differ from the example shown here. The table may not contain very many entries until the malwareattacks script is finished. Use the refresh button periodically to update the table. Also, several Threat Log columns have been hidden in this example.

16. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.10 Create Tags
You can create color-coded labels for use in various places within the firewall web configuration. These
labels can be visual aids that help you more quickly locate information. In this section, you will create
Tags to use with your security policy rules.

1. Select Objects > Tags. Click Add.

These entries indicate that the firewall has blocked access to dangerous URL categories using the URL Filtering profile you defined. Note that several default columns have been hidden in this example.

2. In the Tag window, Enter Allow for the Name. For Color, select Lime. For comments, type Tag for
allowed traffic. Click OK.

3. In the Tags window, click Add again.
4. In the Tag window, Enter Block for the Name. For Color, select Red. For Comments, type Tag for blocked traffic. Click OK.
5. Leave the Palo Alto Networks Firewall open and continue to the next task.