

2. Your organization performs regular network and vulnerability scans from certain hosts which only network security administrators can access. The sfPortscan preprocessor triggers many alerts when these scans take place, yet you know they are not indicative of unauthorized scan activity. Which of the actions below would be best to invoke to reduce the number of false alerts that result from this activity?
 - a. Shut down the sensor picking up these alerts during scheduled scan times.
 - b. Include the IP addresses of the hosts that perform these scans in the Ignore Scanner field of the sfPortscan preprocessor configuration.
 - c. Exclude the IP addresses of the hosts that perform these scans when you query the alert database.
 - d. Include the IP addresses of the hosts that perform these scans in the Ignore Scanned field of the sfPortscan preprocessor configuration.

3. In the process of tuning your network sensors, you can choose to do which of the following?
 - a. Assign pass rules to filter hosts that may be erroneously triggering alerts.
 - b. Use suppression rules to filter sources of noisy alerts.
 - c. Use the thresholding feature to minimize the amount of alerts to more manageable levels.
 - d. All of the above.

4. RNA sensors can save unknown OS data if you choose to do so when you configure an RNA Detection policy. Selecting this option has what effect?
 - a. Protocol banner data for OS's RNA cannot identify is stored in a text file in the /var/sf/RNA directory so you can view the banners and make a manual OS identification.
 - b. The statistical data RNA gathers in the process is stored in a text file on the RNA sensor. Normally, this data is flushed when the OS has been identified, but RNA will keep it indefinitely so you can manually identify the OS yourself.
 - c. RNA will generate a "Unknown OS" event with the IP address of the host it is having trouble identifying.
 - d. RNA stores events related to unidentified operating systems on the RNA Sensor. This data is saved in packet capture (pcap) format and can be found at /var/sf/rna/unknown.pnd on the RNA Sensor.

5. Which of the options listed below cannot be used with the HTTP_Inspect Profile option in the Sourcefire 3D System interface?
 - a. server_flow_depth
 - b. allow_proxy_use
 - c. double_decode
 - d. no_alerts

Answer Key:

1. D | 2. B | 3. D | 4. D | 5. C