Writing a Snort Rule

Snort Detection Rule:

alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"Attack Detected"; flow:to_server,established; content:"|02|";depth:1;content:"sa";depth:2;offset:39; nocase; detection_filter:track_by_src,count 5,seconds 2;)

Analysis:

The detection rule is written to generate an alert when network activity over TCP matches its specifications. Furthermore, part of those specifications includes recognizing when any traffic originates from outside the LAN using any source port and is attempting to initiate a connection (as denoted by ->) with local SQL_SERVERS using destination port 1433.

The msg option tells the engine to print the message Attack Detected when the rule is triggered.

The flow:to_server,established rule option is a non-payload detection rule option. Moreover, the flow keyword allows rules to only apply to certain directions of the traffic flow. to_server means that the rule only triggers on client requests, i.e., on established TCP connections. So, the whole meaning of the option is the rule only triggers when a client has established a TCP connection with the server (The Snort Project, 2013).

content:"|02|";depth:1 is a payload detection option that allows the user to set rules that search for specific content in the packet payload. This option will trigger if the integer 2 is located within the first (1) byte of the payload as the depth option modifier specifies how far into a packet Snort should search for the pattern (The Snort Project, 2013).

content:"sa";depth:2;offset:39; nocase adds 2 additional content option modifiers, offset and nocase. The content option modifier offset allows the rule author to indicate where to start searching for a pattern within a packet. The nocase content option modifier specifies that the Snort should look for the specific pattern, regardless of the case. Together, this section of the rule specifies that the text content sa should be searched for within the first 2 bytes of the payload, however, those first bytes occur 39 bytes into the payload as specified by offset:39 (so bytes 40 & 41 will be checked), lastly, the nocase modifier means sa will be matched regardless of the upper or lower case of s and a.

detection_filter:track_by_src is a post-detection rule option and the detection_filter defines a rate that must be exceeded by a source/destination host before a rule can generate an event. In this case, the rate is tracked using the source IP address (src). Furthermore, the specified rate count 5,seconds 2 means the rule will trigger if more than 5 rule matches occur within any 2-second time period.