Week 8 Task 8.1P

Q1: Consider the following Snort rule:

A. What protocol is this rule applied to?
- The rule is applicable to all IP traffic, irrespective of the protocol used at the transport layer, such as TCP, UDP, or ICMP.

B. What traffic is monitored?
- Source Port: Tracks all traffic coming from a given port.
- Source Address: Tracks network activity coming from any IP address.
- Destination: Keeps track of traffic going to ant IP address.
- Direction: Keeps track of traffic moving from the source to the destination.
- Destination Port: Keep track of traffic to any port of destination

C. What is the rule action?
- The parameter 'alert' instructs Snot to produce an alert if this rule is matched.

D. What does msg: "IP Packet detected" do in this rule?
- "IP packet detected" is the message. This message, which is recorded and shown when the rule user that an IP packet matching the criteria of the rule has been found.

E. What is the meaning of sid:1000002 in this rule?
- '1000002' is the signature ID. Is the rule's special identification. It makes the reference to this particular rule in Snort and other tools cleaner. To prevent inconsistencies with Snort's official rule sets, 'sid' values larger than 1,000,000 are utilize in custom rules.

F. What is the meaning of rev:0 in this rule?
- Version 0 of the rule is denoted by the 'Revision Number' the revision number 'rev' is increased whenever a rule is changed or modified. This rule's initial iteration is indicated by rev: 0

Q2: Consider the following Snort rule:

A. What protocol is this rule applied to?
- TCP traffic is subject to the regulation.

B. What traffic is monitored?
- Source Port: Tracks activity coming from any source port.
- Source Address: Tracks network activity coming from any IP address.
- Destination Address: 192.168.1.0/24 is the range of IP address
- Direction: Keep an eye on traffic moving from the source to the destination.
- Destination Port: Port 23

C. What is the rule action?
- Record: The matched traffic is to be logged, according to this action.

D. Does this rule have a rule option argument?
- The rule option argument is not present in this rule.

Q3: Consider the following Snort rule:

A. What protocol is this rule applied to?
- TCP traffic is subject to the regulation.

B. What traffic is monitored?
- Source Port: Keeps track of all traffic coming from any port.
- Source Address: Tracks networks activity coming from any IP address.
- Destination Address: Keeps track of traffic going to any IP address.
- Direction: Reciprocal <>
- Destination Port: Port 23

C. What is the rule action?
- Record: The matched traffic is to be logged, according to this action.

Q4: Consider the following Snort rule:

A. What protocol is this rule applied to?
    - TCP traffic is subject to the regulation.

B. What traffic is monitored?
    - Source Port: Tracks networks activity coming from any IP address.
    - Source address: Tracks networks activity coming from any IP address.
    - Destination address: Range of IP address is '192.168.1.0/24'
    - Direction: keeps an eye on traffic moving from the source to the destination.
    - Destination Port: Port with the exception of those between 6000 and 6010 !6000:6010

C. What is the rule action?
    - Record: The matched traffic is to be logged, according to this action.

D. What is the meaning of "!6000:6010" in this rule?
    - Negation for the given port range is indicated by the notation '!6000:6010' Traffic to destination ports between '6000' and '6010' is prohibited under the restriction.

Q5: Consider the following Snort rule:

A. What protocol is this rule applied to?
    - TCP traffic is subject to the regulation

B. What traffic is monitored?
    - Source Port: Tracks networks activity coming from any IP address.
    - Source Address: Tracks networks activity coming from any IP address.
    - Destination address: Tracks communication to any IP address as a destination.
    - Direction: Track the flow traffic from the source to the destination.
    - Destination Port: keep track of traffic to any port of destination.

C. What is the rule action?
    - Record: The matched traffic is to be logged, according to this action.

D. What is the meaning of content:"|90|" in this rule?
    - It checks for the hexadecimal byte 0x90 the TCP packets payload contains a content match condition specified by the content |90|

Q6: Consider the following Snort rule:

A. What protocol is this rule applied to?
   - TCP traffic is subject to the regulation.

B. What traffic is monitored?
   - Source Port: Tracks networks activity coming from any IP address.
   - Source Address: Tracks networks activity coming from any IP address.
   - Destination Address: Tracks communication to any IP address as a destination.
   - Direction: keep track of traffic to any port of destination.
   - Destination port: Keeps an eye on traffic going to any port.

C. Keep track of traffic to any port of destination.
   - The parameter 'alert' instructs Snot to produce an alert if this rule is matched.

D. What is the meaning of "offset:40" in this rule?
   - When offset:40 is selected Snort is instructed to begin its search 40 bytes from the packet payload's beginning for the specified content |90|

E. What is the meaning of "depth:75" in this rule?
   - Starting at the offset position (40), the search for the provided content ('|90|') is restricted to the first 75 bytes of the packet payload by using the option "depth:75". This indicates that Snort will examine the payload from byte 40 to byte 115.

Q7:

A. Explain this rule in your own words covering all the different parameters specified as part of it.

- When any of the following requirements are met by a TCP packet, this rule will raise an alert. TCP traffic is tracked in both directions, from the source "$HOME_NET address" and any source port to the destination "$EXTERNAL_NET" from any destination port. The range of ports (6666to7000) on the external network is indicated by the string "6666:7000". The message that will be logged when the rule is triggered is specified in the section '(msg:“CHAT IRC message”;'. The message in this instance will be "CHAT IRC message." "flow:established;": indicates that only connections that have been established should be covered by the rule. It makes sure that only active TCP sessions are taken into account, eliminating connection attempts that are unsuccessful. Content: "PRIVMSG"; indicates the content that has to match within the packet payload. As a common string found in IRC (Internet Relay Chat)communications, it searches for it in this instance. This modifier, "nocase," specifies that case should not be a factor when matching material. sid:1463 This is the rule's special identification, or Snort ID. The rule within Snort's rule set is referenced using it. revision: 6: This provides information on the rule's revision number. It facilitates keeping track of regulation revisions or modifications over time.

Q8: Next week is the final week of tasks in SIT182. It’s a good time to reflect on your journey thus far in SIT182. Think about all the different tasks you have completed and all the hands-on skills you have learned. Similar to other pass-tasks, this question is just a reflection point. How did you learn about Snort rules to complete questions in this task?

- So far, the projects have been equally thrilling and demanding, and each one has improved my comprehension and hands-on experience with a variety of tools utilized in the cyber security industry.