Kieren Ng

Homework 10

4/11/18

1. This rule applies to established connections?

2. The snort rule is monitoring private messages.

3. The traffic needs to between 6666 and 7000 I think.

8.4

User interface- The user can use this to control system behavior and view outputs, etc.

Sensor- collects data, like network packets, system calls, etc.

Analyzer- receives input from sensor, figures out whether an intrusion has occurred

8.8

The base rate fallacy is when people (or systems that people create as well, I guess), is when people tend to choose specific information over general, base information. An example I saw is that a number of intrusions can be low vs the legit users, yet the false alarm rate can be high.

8.2

8.4

a. The rule is an alert to tell if there is an attack at the TCP level (alert tcp). It detects if someone tries to create an Oracle database, and notifies with “ORACLE create database attempt”.

b. If the rule is placed outside the external firewall, it can detect external traffic, whereas I think otherwise it’s just traffic from inside the network.

9.1

If you receive fragments without the first one, you can probably send a request to resend, and you can maybe track the age of the fragments- if the intermediate fragments become too old without a response from the request, then they can be dropped.

9.5

a. Rule A is for incoming mail, if it comes in from outside the firewall and is on 25 then it is allowed, B is for the response from inside the firewall where any port above 1023 is accepted. Rule C is for outgoing mail, if it is on port 25 then it is accepted. Rule D is for the response from outside the firewall, on a port higher than 1023. The last rule just denies everything except for the rules above.

b. Permit, Permit, Permit, Permit

c. Deny, Deny