Components of a detection signature

As a security analyst, you may be tasked with writing, customizing, or testing signatures.
To do this, you'll use IDS tools.
So in this section, we'll examine signature syntax and by the end, you'll be able to read a signature.
A signature specifies detection rules.
These rules outline the types of network intrusions you want an IDS to detect.
For example, a signature can be written to detect and alert on suspicious traffic attempting to connect to a port.
Rule language differs depending on different network intrusion detection systems.
The term network intrusion detection system is often abbreviated as the acronym N-I-D-S and pronounced NIDS.
Generally, NIDS rules consists of three components: an action, a header, and rule options.
Now, let's examine each of these three components in more detail.
Typically, the action is the first item specified in a signature.
This determines the action to take if the rule criteria matches are met.
Actions differ across NIDS rule languages, but some common actions are: alert, pass, or reject.
Using our example, if a rule specifies to alert on suspicious network traffic that establishes an unusual connection to a port, the IDS will inspect the traffic packets and send out an alert.
The header defines the signature's network traffic.
These include information such as source and destination IP addresses, source and destination ports, protocols, and traffic direction.
If we want to detect an alert on suspicious traffic connecting to a port, we have to first define the source of the suspicious traffic in the header.
Suspicious traffic can originate from IP addresses outside the local network.
It can also use specific or unusual protocols.
We can specify external IP addresses and these protocols in the header.
Here's an example of how header information may appear in a basic rule.
First, we can observe that the protocol, TCP, is the first listed item in the signature.
Next, the source IP address 10.120.170.17 and the source port number is specified as being any.
The arrow in the middle of the signature indicates the direction of the network traffic.
So we know it's originating from the source IP 10.120.170.17 from any port going to the following destination IP address 133.113.202.181 and destination port 80.
The rule options lets you customize signatures with additional parameters.
There are many different options available to use.
For instance, you can set options to match the content of a network packet to detect malicious payloads.
Malicious payloads reside in a packet's data and perform malicious activity like deleting or encrypting data.
Configuring rule options helps in narrowing down network traffic, so you can find exactly what

you're looking for.
Typically, rule options are separated by semi-colons and enclosed in parentheses.
In this example, we can examine that the rule options are enclosed in a pair of parentheses and are also separated with semi-colons.
The first rule option, msg, which stands for message, provides the alert's text.
In this case, the alert will print out the text: "This is a message." There's also the option sid, which stands for signature ID.
This attaches a unique id to each signature.
The rev option stands for revision.
Each time a signature is updated or changed, the revision number changes.
Here, the number 1 means it's the first version of the signature.
Great!
Now you've developed another skill in your journey towards becoming a security analyst: how to read signatures.
There's so much more to learn and coming up, we'll discuss tools that use signatures.

Revision #2
Created 2023-11-02 12:44:57 UTC by naruzkurai
Updated 2023-11-02 12:54:12 UTC by naruzkurai