Lab 12.1 Snort Alerts IN715 Networks Three

October 19, 2015

Introduction

Last week we installed and ran Snort in a *packet capture* mode. It simply captured and logged all packets. In a production network setting there would be issues with this. First, we would simply be capturing and logging huge amounts of routine network traffic that has not security significance. Second, there would be security and privacy issues created by creating and holding these logs.

Snort gives us better options. Instead of logging everything, we can use rules to identify and log only those packets that are important in a security context. IN the previous lab we already downloaded and installed a rule set that matches well known patterns of suspicious traffic. We need to understand how those rules are written so that we can evaluate the rules we have adn write our own.

1 Running Snort in NIDS mode

We can start Snort in *Network Intrusion Detection System* (NIDS) mode with a command like

```
snort -dv -l ./log -h 10.25.0.0/16 -c ./snort.conf
```

This tells Snort to verbosely log application layer data (`-dv`) to the file `./log`. It will regard `10.25.0.0/16` as its "home" network and will look for packets matching the rules in `./snort.conf`. We could use the current configuration in `/etc/snort.conf`, but since we would like to work on developing our own rules it makes sense to use our own smaller configuration.

2 Snort rules

Here is an example of a simple Snort rule

```
alert tcp any any -> 10.25.1.50 80 (content:"xml-rpc"; msg: "Possible xml-rpc exploit attempt";)
```

This rule will trigger an *alert* message from any source ip address and port (the two occurances of "`any`") addressed to port 80 on the host at `10.25.1.50` whith the string "`xml-rpc` " in the packet data. When it identifies a matching packet it wil include the message "Possible xml-rpc exploit attempt" in the alert.

You can test rules like this one by putting them in a ocnfiguration file that you specify on the command line as shown above. Write a rule that catches attempted ssh logins. Can you modify it so that it only catches attempted root logins? What about logins only from `10.25.0.0/16`? (Why might you care about those?)

3 Output formats

Snort supports a variety of output formats. Smoe are faster to write, which is important, while others provide more information or information in a more readable format. Two human-readable formats at `alert_full` and `alert_fast`. In your configuration you can specify them like this:

```
output alert_full: [<filename> [<limit>]]
```

Where the optional filename specifies where to write the log, and the optional limit restricts the file to a maximum size, e.g. 512M. Experiment with output formats to see how they work.

4 More information

More information about writing and sing rules is available in the Snort Users' Manual at `http://manual.snort.org/node1.html`, in particular in sections 1 and 3.