GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Webinar: Snort rules

Exercises

017 TU AYUDA EN CIBERSEGURIDAD
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

INDEX

1. PRACTICAL EXERCISE

The objective of the exercise is to improve the rules proposed in the examples of rule creation.

On the one hand, the rule for detecting traffic to the Facebook web pages. And on the other hand, rules to detect IRC traffic in our organization.

Users should research their creation and answer the following questions:

- Is it possible to search only the domain in the HTTP headers? Apply to the Facebook rule.
- Is it possible to create more complex searches than just text or hexadecimal values? Apply to the IRC rule.

Resolution of the exercise:

You can use the keyword "`uricontent`" instead of "`content`" when searching only for the URI of the HTTP requests.

The rule would look like this:

```
log tcp $HOME_NET any -> $EXTERNAL_NET any (msg: “Conexión a Facebook”; uricontent: “facebook.com”; sid:1000001)
```

In the case of IRC, it is possible to make regular expressions when consulting the content. For example, to look for several IRC commands in the same rule we could do the following:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 6666:7000 (msg: “Conexión a servidor IRC”; pcre: “/(JOIN|NICK|SERVER)/”; sid:1000002)
```

2. RESEARCH EXERCISE

How could Snort be used to adjust the values of the rule that detects errors in access to FTP servers and if the source server is 10.0.0.250, this rule is not executed since that server is a honeypot.

Hint: check the "threshold.conf" configuration file that comes with Snort by default.

Resolution of the exercise:

You would have to add a new configuration line to our "threshold.conf" file with the following data:

```
suppress gen_id 1, sig_id 1000003, track by_src, ip 10.0.0.250
```

This line removes the rule 1000003 for the source ip 10.0.0.250.