Practical Network Defense - Lab 7

Suricata on ACME co.

Alessandro Serpi - 1647244

3 May 2019

Contents

1 Introduction

An intrusion prevention systems (IPS) is a device that monitors a network to identify malicious activities, log information about them, report them and attempt to block them. The IPS that comes with OPNsense is Suricata, owned and supported by the Open Information Security Foundation (OISF), a non-profit foundation.

In this laboratory, Suricata is configured in both firewalls to block the majority of suspect or potentially undesired activities (such as the Tor protocol and connections to social networks) and auto-update itself.

2 IPS configuration

In *System* ▷ *Services* ▷ *Intrusion detection* ▷ *Administration*, section *Settings*, tick *Enabled* and *IPS mode* and select all interfaces in the setting of the same name.

In section *Download*, tick all checkboxes and click *Enable (drop filter)*. Then, download and update the rules clicking on the specific button.

In section *Rules*, verify that there are enabled rules. In order to increase performances, only the most prominent rules are enabled by default: Suricata is a highly memory-consuming applicative, enabling all rules would greatly affect network latencies.

In section *Schedule*, set the rules to auto-update every day at midnight. Tick the checkbox, set `0` to *Hours* and *Minutes* and `*` to all others time-related settings.

3 Custom rule writing and description

3.1 EICAR string

EICAR (European Institute for Computer Antivirus Research), together with CARO (Computer Antivirus Research Organization), developed the EICAR test file: a harmless string designed to test the integrity of security software. Compliant applications treat the string as malicious content; in this case, the IPS blocks unencrypted TCP and UDP packets that contain the string.

3.2 Rules

The rules are (ordered by `sid`):

```
drop udp any any -> any any (msg:"EICAR string UDP message";
↪  content:"|58 35 4f 21 50 25 40 41 50 5b 34 5c 50 5a 58 35 34 28 50
↪  5e 29 37 43 43 29 37 7d 24 45 49 43 41 52 2d 53 54 41 4e 44 41 52 44
↪  2d 41 4e 54 49 56 49 52 55 53 2d 54 45 53 54 2d 46 49 4c 45 21 24 48
↪  2b 48 2a|"; classtype:bad-unknown; sid:9900001; rev:1;)
```

```
drop tcp any any -> any any (msg:"EICAR string TCP message";
↪   content:"|58 35 4f 21 50 25 40 41 50 5b 34 5c 50 5a 58 35 34 28 50
↪   5e 29 37 43 43 29 37 7d 24 45 49 43 41 52 2d 53 54 41 4e 44 41 52 44
↪   2d 41 4e 54 49 56 49 52 55 53 2d 54 45 53 54 2d 46 49 4c 45 21 24 48
↪   2b 48 2a|"; flow:established; classtype:bad-unknown; sid:9900002;
↪   rev:1;)
```

The protocol is written in red; it is UDP for the first rule, TCP for the second one. Since the UDP `pcap` file is less complex, the corresponding rule was created first.

The right-facing arrow states that the packets are checked only in one direction. Since the rules are checked against every packet, irregardless of its origin or destination (addresses and ports are in blue), it is useless to specify a bidirectional check.

Options are between parentheses. `msg` is the rule description. `content` states which byte sequence (vertical bars delimit a sequence of bytes in hexadecimal form) the payload must have. `flow` applies only to TCP packet exchanges; it specifies that the packet must belong to an already-established connection. `classtype` is the rule type; since a test class does not exist, it was chosen a generic type. `sid` is the signature id; it must be unique. `rev` is the signature version; since the rules have not been updated yet, it is 1.

3.3 Rule installation

Since OPNsense does not allow to add new rules, it is necessary to create a downloadable ruleset in a web server and manually insert the definition file into the appropriate folder in both firewalls.

First, create the file `custom.rules` with the two rules for the EICAR string in directory `var/www/html/suricata` of host `web.pndeflab.edu`, the only web server in this laboratory. Then, add the ruleset `Custom/custom` manually inserting the file `custom.xml`:

```xml
<?xml version="1.0"?>
<ruleset documentation_url="http://docs.opnsense.org/">
    <location url="http://web.pndeflab.edu/suricata/" prefix="Custom"/>
    <files>
        <file description="custom">custom.rules</file>
    </files>
</ruleset>
```

in the directory `/usr/local/opnsense/scripts/suricata/metadata/rules` of both firewalls.

4 Test of the rules

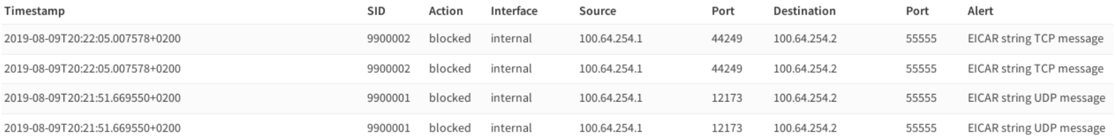
Testing was performed manually, opening a terminal in both firewalls and trying to send the EICAR string using *netcat*. The default policies were momentarily changed to allowing all incoming packets to avoid false negatives.

For TCP, the pair of commands was:

```
nc -l 55555  # server
echo "$EICAR_STRING" | nc $OTHER_FIREWALL 55555  # client
```

For UDP is identical, except for the flag `-u`.

The packets were never received by the server because they were blocked by the client, as showed by the alerts.



Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert
2019-08-09T20:22:05.007578+0200	9900002	blocked	internal	100.64.254.1	44249	100.64.254.2	55555	EICAR string TCP message
2019-08-09T20:22:05.007578+0200	9900002	blocked	internal	100.64.254.1	44249	100.64.254.2	55555	EICAR string TCP message
2019-08-09T20:21:51.669550+0200	9900001	blocked	internal	100.64.254.1	12173	100.64.254.2	55555	EICAR string UDP message
2019-08-09T20:21:51.669550+0200	9900001	blocked	internal	100.64.254.1	12173	100.64.254.2	55555	EICAR string UDP message

5 Final remarks

IPSs offer an invaluable service to system administrators, allowing them to enforce specific policies and stop 0-day attacks while waiting for a patch. However, they require a great amount of resource to run smoothly without hindering the network. Deciding which rule enable is more an art than a science, while surely being a full-time job that may be challenging even for the most experienced sysadmin.

In this regard, OPNsense greatly simplifies the task of selecting the most common rules, however, it removes all advanced tools: there is no straightforward way to add custom rules or new rulesets, affecting the immediate response to new threats.