LAB: snort (IDS)

Lab Environment

The workshop WiFi:

- SSID: `workshop`
- PASS: `iij/2497`

Hosts - Virtual machines (Ubuntu 18.04LTS/LXC)

- Hostname: `nsXX.workshop`
- IPv6: `fd00:2497:1::X`
- IPv4: `10.0.0.X`

Where `X` and `XX` is yoru group ID. For group 1, hostname is `ns01.workshop`, IPv6 address is `fd00:2497:1::1`, and IPv4 is `10.0.0.1`.

Install and configure snort

Login using `ssh` to your virtual server and install snort.

```
$ sudo apt install snort
```

The installer will ask you the target network to monitor. For this lab, just specify your virtual server address.

```
10.0.0.X/32
```

Where `X` is your group ID. This is set to the `HOME_NET` variable which can be used in the configuration file. This doesn't mean you cannot monitor other addresses.

Update configuration file

The main configuration file is at `/etc/snort/snort.conf`.

To enable alert log, comment the following line (insert `#` at the head of the line).

```
output unified2: filename snort.log, limit 128, nostamp, mpls_event_types, vlan_ev
ent_types
```

To avoid strict checksum verification mode, change the value of `checksum_mode` from `all` to `none`.

```
config checksum_mode: none
```

To make it easy to check our modification, disable all the rules predefined in the `snort.conf` for this lab. There are many rule definitions in the `/etc/snort/rules/` directory. Comment all the lines starting as `include $RULE_PATH` except `include $RULE_PATH/local.rules` in the `snort.conf` file.

The file `/etc/snort/rules/local.rules` is the file we use to add our own rules in this lab.

Exercise 1: Stupid rule

Add the following rule into `/etc/snort/rules/local.rules`.

```
alert ip any any -> any any (msg: "IP Packet detected"; sid: 1000000;)
```

Restart the snort service.

```
$ sudo systemctl restart snort
```

Check the `/var/log/snort/alert` file to see what kind of messages are recorded.

```
$ sudo tail -f /var/log/snort/alert
```

Once you have confirmed that the snort and your local rule are working correctly, you can remove this stupid rule since it is a bit annoying to show alert messages for all the incoming IP packets.

Exercise 2: XMAS scan rule

Try to write a new rule to detect the XMAS scan (https://nmap.org/book/scan-methods-null-fin-xmas-scan.html).

> Hint: The XMAS scan sets the TCP FIN, PSH, and URG flags. Check the `flags` rule.

Once you've written your rule and restarted the snort service, check if the rule is working using the `nmap` command from your local computer, or ask your neighbors to scanp your virtual server from their terminals.

```
$ sudo nmap -sX YOUR_VIRTUAL_SERVER_ADDRESS
```

> Note: You cannot verify your rules from inside your virtual server, since all the packets sent from your server to your server go to the loopback interface (`lo`), not the interface that the snort service is monitoring (`eth0`)

Exercise 3: Web access

Try to write a new rule to detect that someone access to a specific web page of your web server.

> Hint: The content of the packet can be checked using the `content` rule.

Exercise 4: Detect ssh brute force attack

Try to write a new rule to detect the ssh brute force attack. The condition is 'more than 3 connection in 60 seconds'.

> Hint: The `threshold` rule.