Getting Started With CrowdSec

Team:

R Tarun

Under The Guidance: Dr. Sibi Chakkaravarthy Sethuraman

Center of Excellence in Cyber Security, VIT-AP University

CONTENTS

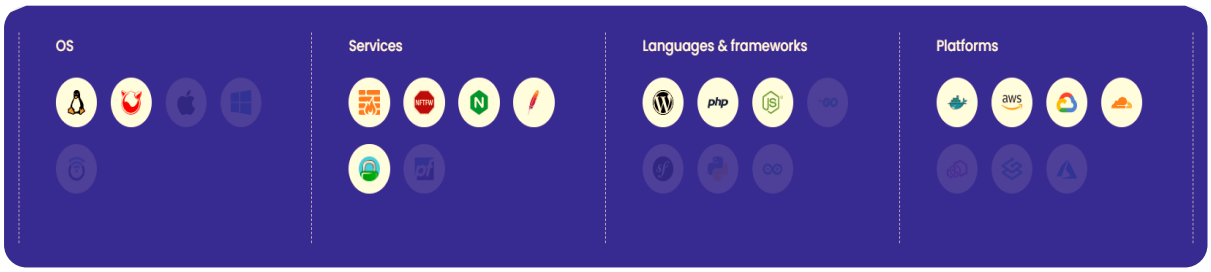
What Is CrowdSec?

CrowdSec is a free, open-source and collaborative IPS.

Analyze behaviors, respond to attacks & share signals across the community.

How does it work?

Where To Use It?



Examples Of Detected Behaviour's

Getting Started

Prerequisites

- Ubuntu/Windows server
- Apache2 or any service installed in server
- If(server == ubuntu) Convert CLI to GUI
  (Command: `sudo apt install ubuntu-desktop`) **[OPTIONAL]**

How To Install (In Ubuntu)

1. Open terminal
2. Installing CrowdSec repositories, allows you to access the latest packages of crowdsec and bouncers which can be done by following command: `curl -s https://packagecloud.io/install/repositories/crowdsec/crowdsec/script.deb.sh | sudo bash`
3. Now you need to install crowdsec from the following command:
   `sudo apt install crowdsec`
4. CrowdSec's detection capabilities provide observability on what is going on. However, to protect yourself, you need to block attackers, which is where bouncers play a major part. Remember: CrowdSec detects, bouncers deter. Now you need to install a bouncer with the following commands.
   `sudo apt install crowdsec-firewall-bouncer-iptables`
   `sudo apt install crowdsec-firewall-bouncer-nftables`
5. Now you need to enable the services of crowdsec by the following command.
   `Sudo /usr/share/crowdsec/wizard.sh -c`
6. A parser is a YAML configuration file that describes how a string is being parsed. Said string can be a logline, or a field extracted from a previous parser. You can view the list of parsers by entering the following command.
   `cscli parsers list`
   Whitelist parser is configured by default in CrowdSec which is responsible for not blocking suspicious ip's. It should be removed as we need our model to detect and block the suspicious ip's, can be done by following command
   `sudo cscli parsers remove crowdsecurity/whitelists`
   `sudo systemstl reload crowdsec`

Verify your installation

1. Verify your server installation by pinging your server ip, can be done by opening terminal/command prompt of the parent machine and ping the ip of your server.
   Ex: `ping 192.168.11.133`
2. Check status of installed services by running following commands in your server:
   `Sudo systemctl status apache2`
   `Sudo systemctl status crowsec`

Verify the defenses of your server (By SSH_Brute_Force)

1. In the terminal of your server, open the live log of crowsec by running the following command. **[FIG 1]**
   `sudo tail -f /var/log/crowdsec.log`
2. Now go to another virtual machine, open terminal and try to ssh connect the server by entering the wrong password by the following command. **[FIG 2]**
   `ssh [servername]@[server ip]`
   `Ex: ssh kiyo@192.168.11.133`

3. Now after 3 attempts to login you'll get blocked as crowdsec detects as ssh bruteforce is being made to check that you need to go back to server terminal where you can find freshly generated text in your log file. **[FIG 3]**
4. You can also verify that by running the following command**. [FIG 4]**
   `sudo cscli decisions list`

Representations

FIG 1

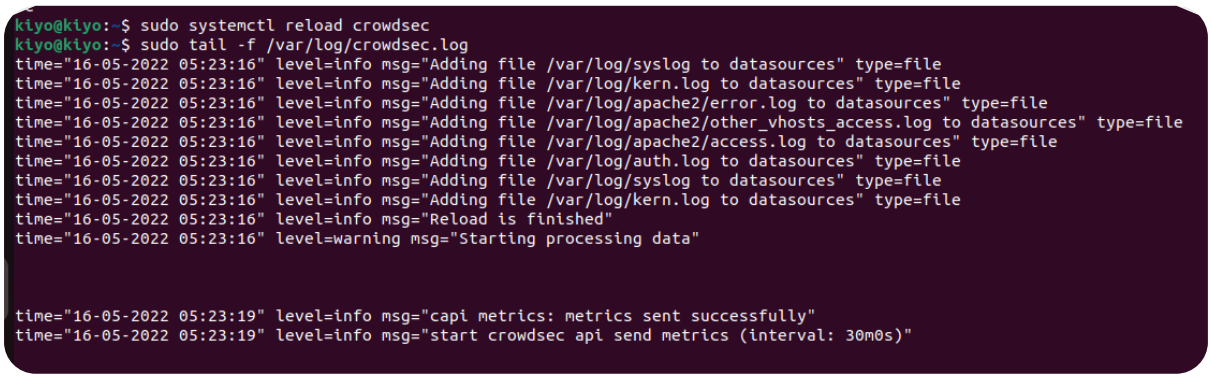


FIG 2

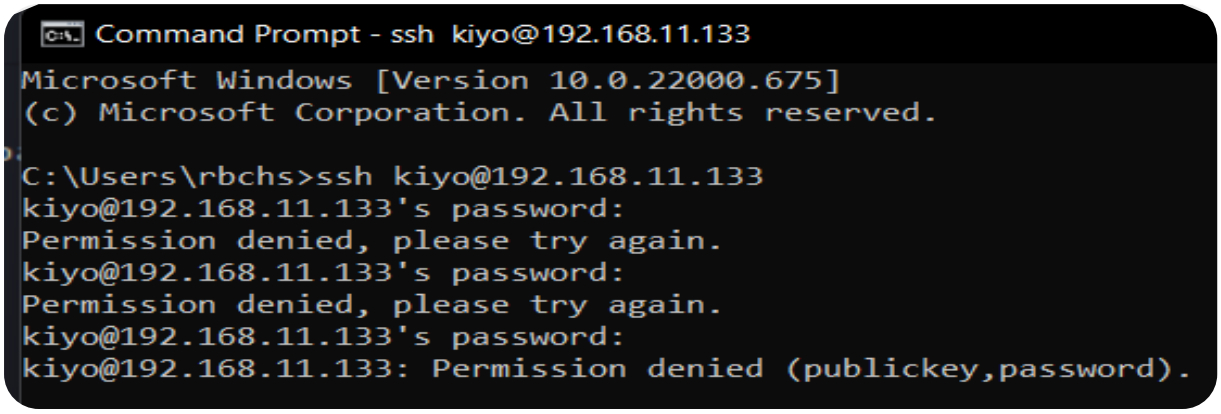


FIG 3

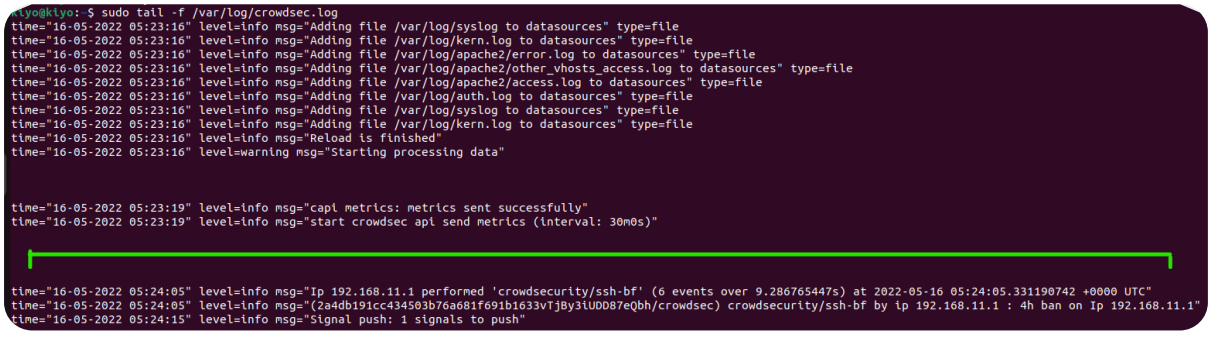
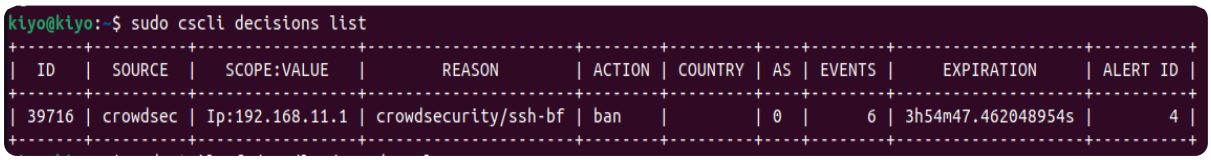


FIG 4



Verify the defenses of your server (By Nikto_Tool)

1. In the terminal of your server, open the live log of crowsec by running the following command. **[FIG 1]**
   ```
   sudo tail -f /var/log/crowdsec.log
   ```
2. Now go to another virtual machine, open the terminal and open the nikto tool, and run the following Command **[FIG 2]**
   ```
   ssh nikto -h [server ip]
   Ex: nikto -h 192.168.11.131
   ```
3. Now in the middle the scan takes long time and couldn't get complete as our machine blocked by crowdsec as crowd sec detects and block the vulnerability scanners. Mean while go to our server log to check the behavior of crowdsec **[FIG 3]**
4. You can also verify that by running the following commands**. [FIG 4.1]**
   ```
   sudo cscli decisions list
   sudo cscli alerts list
   ```

Representations

FIG 1

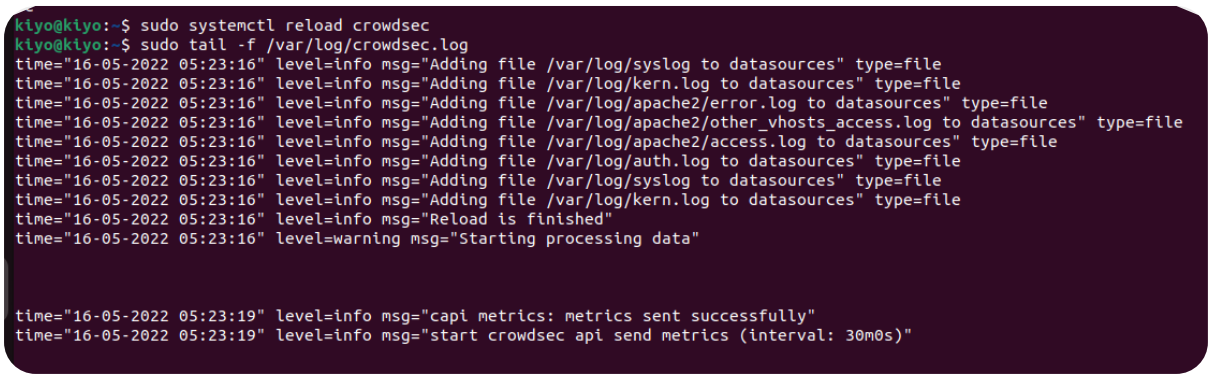


FIG 2

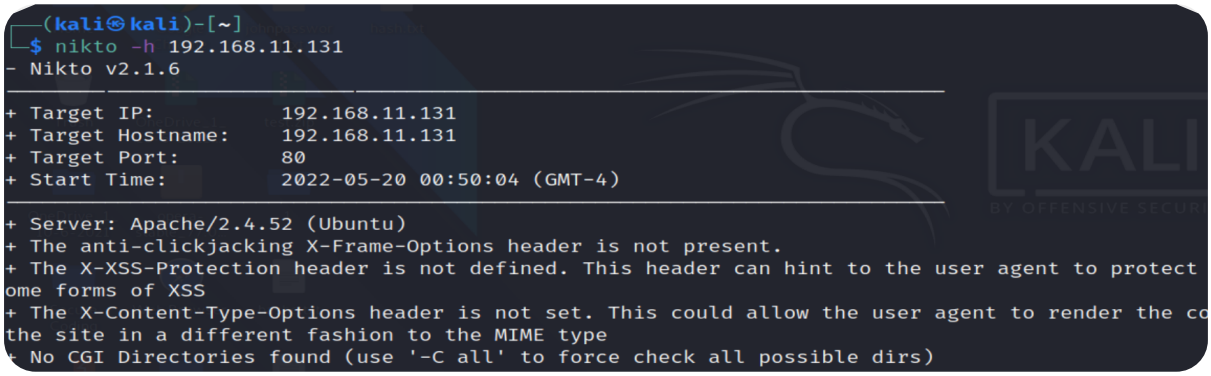


FIG 3

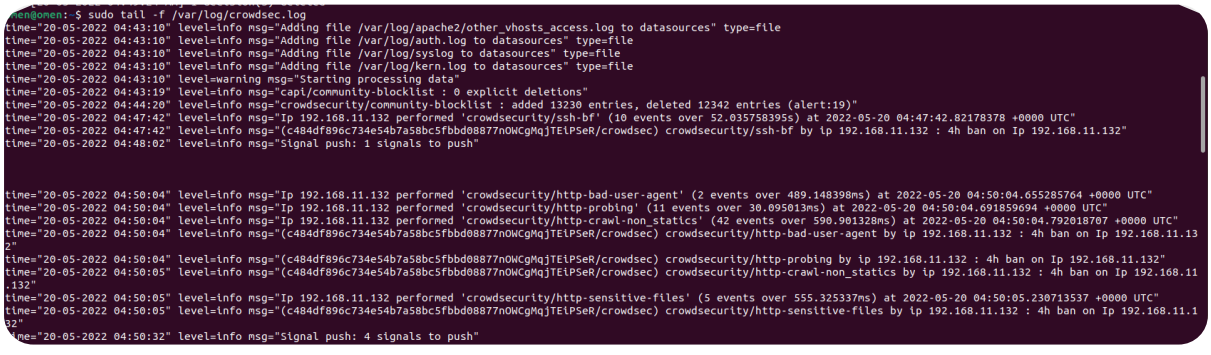
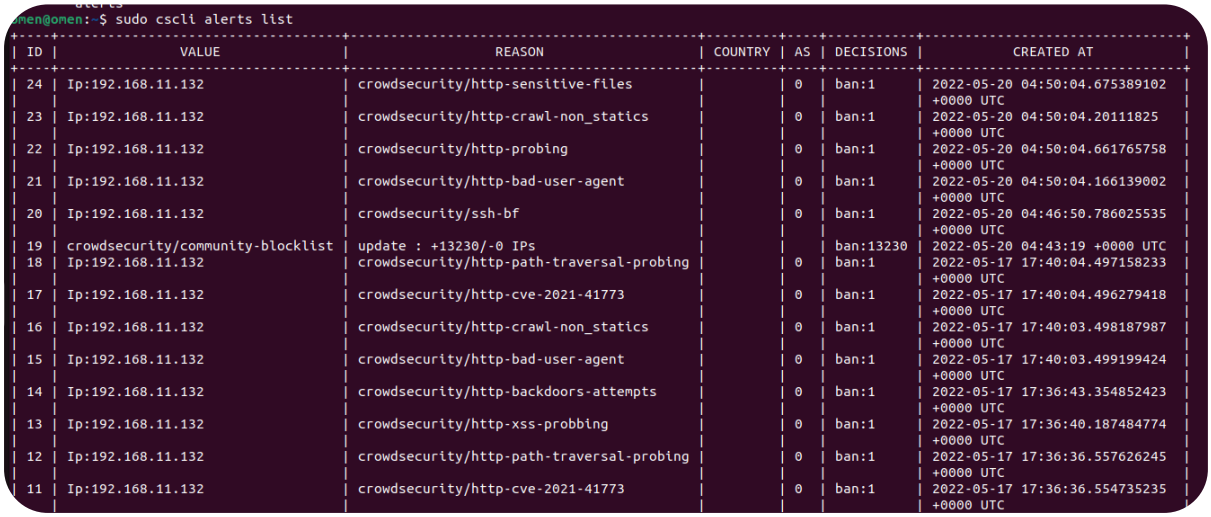


FIG 4



```
men@omen:~$ sudo cscli alerts list
+----+----------------------------------+----------------------------------------+---------+----+-----------+-------------------------------+
| ID |              VALUE               |                REASON                  | COUNTRY | AS | DECISIONS |          CREATED AT           |
+----+----------------------------------+----------------------------------------+---------+----+-----------+-------------------------------+
| 24 | Ip:192.168.11.132                | crowdsecurity/http-sensitive-files     |         | 0  | ban:1     | 2022-05-20 04:50:04.675389102 |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
| 23 | Ip:192.168.11.132                | crowdsecurity/http-crawl-non_statics   |         | 0  | ban:1     | 2022-05-20 04:50:04.20111825  |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
| 22 | Ip:192.168.11.132                | crowdsecurity/http-probing             |         | 0  | ban:1     | 2022-05-20 04:50:04.661765758 |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
| 21 | Ip:192.168.11.132                | crowdsecurity/http-bad-user-agent      |         | 0  | ban:1     | 2022-05-20 04:50:04.166139002 |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
| 20 | Ip:192.168.11.132                | crowdsecurity/ssh-bf                   |         | 0  | ban:1     | 2022-05-20 04:46:50.786025535 |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
| 19 | crowdsecurity/community-blocklist | update : +13230/-0 IPs                 |         |    | ban:13230 | 2022-05-20 04:43:19 +0000 UTC |
| 18 | Ip:192.168.11.132                | crowdsecurity/http-path-traversal-probing |      | 0  | ban:1     | 2022-05-17 17:40:04.497158233 |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
| 17 | Ip:192.168.11.132                | crowdsecurity/http-cve-2021-41773      |         | 0  | ban:1     | 2022-05-17 17:40:04.496279418 |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
| 16 | Ip:192.168.11.132                | crowdsecurity/http-crawl-non_statics   |         | 0  | ban:1     | 2022-05-17 17:40:03.498187987 |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
| 15 | Ip:192.168.11.132                | crowdsecurity/http-bad-user-agent      |         | 0  | ban:1     | 2022-05-17 17:40:03.499199424 |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
| 14 | Ip:192.168.11.132                | crowdsecurity/http-backdoors-attempts  |         | 0  | ban:1     | 2022-05-17 17:36:43.354852423 |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
| 13 | Ip:192.168.11.132                | crowdsecurity/http-xss-probbing        |         | 0  | ban:1     | 2022-05-17 17:36:40.187484774 |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
| 12 | Ip:192.168.11.132                | crowdsecurity/http-path-traversal-probing |      | 0  | ban:1     | 2022-05-17 17:36:36.557626245 |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
| 11 | Ip:192.168.11.132                | crowdsecurity/http-cve-2021-41773      |         | 0  | ban:1     | 2022-05-17 17:36:36.554735235 |
|    |                                  |                                        |         |    |           | +0000 UTC                     |
```

Basics To Handle CrowdSec

- `sudo cscli hub list`

This lists installed parsers, scenarios and/or collections.
They represent what your CrowdSec setup can parse (logs) and detect (scenarios).
Adding `-a` will list all the available configurations in the hub.

- `sudo cscli <configuration_type> install <item>`

`configuration_type` can be `collections`, `parsers`, `scenarios` or `postoverflows`.
You are most likely to only install collections that contain the needed parsers and scenarios to cover a technical stack :

```
sudo cscli collections install crowdsecurity/nginx
```

- `sudo cscli hub updatesudo cscli hub upgrade`

This will upgrade your existing parsers, scenarios and collections to the latest available version. You can as well use a more granular approach like

`sudo cscli <configuration_type> upgrade <item>`.

`configuration_type` can be `parsers`, `scenarios`, `collections`, `hub` or `postoverflows`.

- `sudo cscli decisions list`

If you just deployed CrowdSec, the list might be empty, but don't worry, it simply means you haven't yet been attacked, congrats! Adding `-a` flag will as well list the decisions you received from the community blocklist.

- `cscli decisions add -i 1.2.3.4cscli decisions delete -i 1.2.3.4`

Those commands will respectively add a manual decision for ip `1.2.3.4` (with default parameters such as duration and such), and remove all active decisions for ip `1.2.3.4`.

- `sudo cscli alerts list`

While decisions won't be shown anymore once they expire (or are manually deleted), the alerts will stay visible, allowing you to keep track of past decisions. You will here see the alerts, even if the associated decisions expired.

- `sudo cscli metrics`

The metrics displayed are extracted from CrowdSec prometheus.

- `sudo tail -f /var/log/crowdsec.log`

  `/var/log/crowdsec.log` is the main log, it shows ongoing decisions and acquisition/parsing/scenario errors.

  `/var/log/crowdsec_api.log` is the access log of the local api (LAPI)

- Ban an IP

```
sudo cscli decisions add -i 1.2.3.4
```

- Add a decision (ban) on IP `1.2.3.4` for 24 hours, with reason 'web bruteforce'

```
sudo cscli decisions add --ip 1.2.3.4 --duration 24h --reason "web bruteforce"
```

- Add a decision (ban) on range `1.2.3.0/24` for 4 hours, with reason 'web bruteforce'

```
sudo cscli decisions add --range 1.2.3.0/24 --reason "web bruteforce"
```

- Add a decision (captcha) on ip `1.2.3.4` for 4hours (default duration), with reason 'web bruteforce'

```
sudo cscli decisions add --ip 1.2.3.4 --reason "web bruteforce" --type captcha
```