

Getting Started With CrowdSec

Team:

R Tarun

Under The Guidance: Dr. Sibi Chakkaravarthy Sethuraman
Center of Excellence in Cyber Security, VIT-AP University



CONTENTS

- 1. What is CrowdSec?**
- 2. How does it work?**
- 3. Where To Use It?**
- 4. Examples Of Detected Behaviors**
- 5. Getting Started**
- 6. Prerequisites**
- 7. How To Install (In Ubuntu)**
- 8. Verify your installation**
- 9. Verify the defenses of your server (By
SSH_Brute_Force)**
- 10. Verify the defenses of your server (By
Nikto_Tool)**
- 11. Basics To Handle CrowdSec**

CrowdSec is a free, open-source and collaborative IPS.
Analyze behaviors, respond to attacks & share signals across the community.

Set up your own intrusion detection system

Apply behavior scenarios to identify cyberthreats

Parse logs

Acquire data from any source (syslog, cloudtrails, SIEM, etc.)

Automate your security

Define the type of remediation you want to apply and where

Leverage the community's IP blocklist

Share and benefit from a crowdsourced and curated cyber threat intelligence system

The diagram illustrates the relationship between four categories of technology, each represented by a set of icons in a grid. The categories are separated by vertical dashed lines.

- OS:** Includes icons for Linux (Tux penguin), macOS (Fire logo), Apple (Apple logo), Windows (Windows logo), and Android (Android robot).
- Services:** Includes icons for IBM, Netflix, Google (G logo), and a red pencil icon, followed by a blue cloud icon and a blue square icon.
- Languages & frameworks:** Includes icons for WordPress, PHP, JavaScript (JS logo), and a blue infinity symbol, followed by a blue infinity symbol, a blue infinity symbol, and a blue infinity symbol.
- Platforms:** Includes icons for Google Cloud (GCP logo), AWS, Google Cloud (GCP logo), and a blue cloud icon, followed by a blue infinity symbol, a blue infinity symbol, and a blue infinity symbol.

The diagram consists of a 3x3 grid of hexagonal icons, each representing a different type of cyber threat. The icons are as follows:

- Top Row:**
 - Applicative DDoS:** An icon showing three server racks with three bombs flying towards them.
 - Drive by download:** An icon of a web browser window with a bug inside.
 - Resource abuse:** An icon of a water faucet with a single drop of water falling from it.
- Middle Row:**
 - Credentials Brute-forcing:** An icon of a padlock with four asterisks below it.
 - PHP-based armageddons:** An icon of a nuclear mushroom cloud.
 - Port scans:** An icon showing a grid of numbers (21, 22, 23, 25, 80) with a magnifying glass over the number 22.
 - Web scans:** An icon of a smartphone and a tablet.
- Bottom Row:**
 - Credential stuffing:** An icon of a credit card with a padlock over it.
 - Bot scraping:** An icon of a web browser window with a bot icon and a warning triangle.
 - Targeted attacks:** An icon of a person inside a target symbol.

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.
`csccli 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 csccli parsers remove crowdsecurity/whitelists`
`sudo systemctl 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 crowdsec`

Verify the defenses of your server (By SSH_Brute_Force)

1. In the terminal of your server, open the live log of crowdsec 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`

- Now after 3 attempts to login you'll get blocked as crowdsec detects as ssh brute force 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]**
- You can also verify that by running the following command. **[FIG 4]**
`sudo cscli decisions list`

Representations

FIG 1

```
kiyo@kiyo:~$ sudo systemctl reload crowdsec
kiyo@kiyo:~$ sudo tail -f /var/log/crowdsec.log
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/syslog to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/kern.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/apache2/error.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/apache2/other_vhosts_access.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/apache2/access.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/auth.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/syslog to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/kern.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Reload is finished"
time="16-05-2022 05:23:16" level=warning msg="Starting processing data"

time="16-05-2022 05:23:19" level=info msg="capi metrics: metrics sent successfully"
time="16-05-2022 05:23:19" level=info msg="start crowdsec api send metrics (interval: 30m0s)"
```

FIG 2

```
C:\%> Command Prompt - ssh kiyo@192.168.11.133
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

C:\Users\rbchs>ssh kiyo@192.168.11.133
kiyo@192.168.11.133's password:
Permission denied, please try again.
kiyo@192.168.11.133's password:
Permission denied, please try again.
kiyo@192.168.11.133's password:
kiyo@192.168.11.133: Permission denied (publickey,password).
```

FIG 3

```
kiyo@kiyo:~$ sudo tail -f /var/log/crowdsec.log
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/syslog to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/kern.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/apache2/error.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/apache2/other_vhosts_access.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/apache2/access.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/auth.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/syslog to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/kern.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Reload is finished"
time="16-05-2022 05:23:16" level=warning msg="Starting processing data"

time="16-05-2022 05:23:19" level=info msg="capi metrics: metrics sent successfully"
time="16-05-2022 05:23:19" level=info msg="start crowdsec api send metrics (interval: 30m0s)"

time="16-05-2022 05:24:05" level=info msg="Ip 192.168.11.1 performed 'crowdsecurity/ssh-bf' (6 events over 9.286765447s) at 2022-05-16 05:24:05.331190742 +0000 UTC"
time="16-05-2022 05:24:05" level=info msg="(2a4db191cc434503b76a681f691b1633vj3y3lU0D07eQbh/crowdsec) crowdsecurity/ssh-bf by ip 192.168.11.1 : 4h ban on Ip 192.168.11.1"
time="16-05-2022 05:24:15" level=info msg="Signal push: 1 signals to push"
```

FIG 4

```
kiyo@kiyo:~$ sudo cscli decisions list
```

ID	SOURCE	SCOPE:VALUE	REASON	ACTION	COUNTRY	AS	EVENTS	EXPIRATION	ALERT ID
39716	crowdsec	Ip:192.168.11.1	crowdsecurity/ssh-bf	ban		0	6	3h54m47.462048954s	4

Verify the defenses of your server (By Nikto_Tool)

1. In the terminal of your server, open the live log of crowdsec 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

```
k1yo@k1yo:~$ sudo systemctl reload crowdsec
k1yo@k1yo:~$ sudo tail -f /var/log/crowdsec.log
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/syslog to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/kern.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/apache2/error.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/apache2/other_vhosts_access.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/apache2/access.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/auth.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/syslog to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Adding file /var/log/kern.log to datasources" type=file
time="16-05-2022 05:23:16" level=info msg="Reload is finished"
time="16-05-2022 05:23:16" level=warning msg="Starting processing data"

time="16-05-2022 05:23:19" level=info msg="capi metrics: metrics sent successfully"
time="16-05-2022 05:23:19" level=info msg="start crowdsec api send metrics (interval: 30m0s)"
```

FIG 2

```
(kali㉿kali)-[~]
└─$ nikto -h 192.168.11.131
- Nikto v2.1.6

+ Target IP: 192.168.11.131
+ Target Hostname: 192.168.11.131
+ Target Port: 80
+ Start Time: 2022-05-20 00:50:04 (GMT-4)

+ Server: Apache/2.4.52 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
ome forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the co
the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

FIG 3

```
andromeda:~$ sudo tail -f /var/log/crowdsec.log
time="20-05-2022 04:43:10" level=info msg="Adding file /var/log/apache2/other_vhosts_access.log to datasources" type=file
time="20-05-2022 04:43:10" level=info msg="Adding file /var/log/auth.log to datasources" type=file
time="20-05-2022 04:43:10" level=info msg="Adding file /var/log/syslog to datasources" type=file
time="20-05-2022 04:43:10" level=info msg="Adding file /var/log/kern.log to datasources" type=file
time="20-05-2022 04:43:10" level=warning msg="Starting processing data"
time="20-05-2022 04:43:19" level=info msg="capi/community-blocklist : 0 explicit deletions"
time="20-05-2022 04:44:20" level=info msg="crowdsecurity/community-blocklist : added 13230 entries, deleted 12342 entries (alert:19)"
time="20-05-2022 04:47:42" level=info msg="Ip 192.168.11.132 performed 'crowdsecurity/ssh-bf' (10 events over 52.035758395s) at 2022-05-20 04:47:42.82178378 +0000 UTC"
time="20-05-2022 04:47:42" level=info msg="(c484df896c734e54b7a58bc5fbbd08877n0McGmQJTElP5eR/crowdsec) crowdsecurity/ssh-bf by Ip 192.168.11.132 : 4h ban on Ip 192.168.11.132"
time="20-05-2022 04:48:02" level=info msg="Signal push: 1 signals to push"

time="20-05-2022 04:50:04" level=info msg="Ip 192.168.11.132 performed 'crowdsecurity/http-bad-user-agent' (2 events over 489.148398ms) at 2022-05-20 04:50:04.655285764 +0000 UTC"
time="20-05-2022 04:50:04" level=info msg="Ip 192.168.11.132 performed 'crowdsecurity/http-probing' (11 events over 30.095013ms) at 2022-05-20 04:50:04.691859694 +0000 UTC"
time="20-05-2022 04:50:04" level=info msg="Ip 192.168.11.132 performed 'crowdsecurity/http-crawl-non-statics' (42 events over 590.901328ms) at 2022-05-20 04:50:04.792018707 +0000 UTC"
time="20-05-2022 04:50:04" level=info msg="(c484df896c734e54b7a58bc5fbbd08877n0McGmQJTElP5eR/crowdsec) crowdsecurity/http-bad-user-agent by Ip 192.168.11.132 : 4h ban on Ip 192.168.11.132"
time="20-05-2022 04:50:04" level=info msg="(c484df896c734e54b7a58bc5fbbd08877n0McGmQJTElP5eR/crowdsec) crowdsecurity/http-probing by Ip 192.168.11.132 : 4h ban on Ip 192.168.11.132"
time="20-05-2022 04:50:05" level=info msg="(c484df896c734e54b7a58bc5fbbd08877n0McGmQJTElP5eR/crowdsec) crowdsecurity/http-crawl-non-statics by Ip 192.168.11.132 : 4h ban on Ip 192.168.11.132"
time="20-05-2022 04:50:05" level=info msg="Ip 192.168.11.132 performed 'crowdsecurity/http-sensitive-files' (5 events over 555.325337ms) at 2022-05-20 04:50:05.230713537 +0000 UTC"
time="20-05-2022 04:50:05" level=info msg="(c484df896c734e54b7a58bc5fbbd08877n0McGmQJTElP5eR/crowdsec) crowdsecurity/http-sensitive-files by Ip 192.168.11.132 : 4h ban on Ip 192.168.11.132"
time="20-05-2022 04:50:32" level=info msg="Signal push: 4 signals to push"
```

FIG 4

```
ngmonen:~$ 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-probing		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 1.2.3.4``cscli 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
```