fast.log

```
tiago-paquete@Linux:~$ curl http://testmynids.org/uid/index.html
==========================================================================
uid=0(root) gid=0(root) groups=0(root)
==========================================================================
```

This output mimics a **command execution result**, making it look like an **attacker got root**. This is **not malicious** but a **test page** specifically made to trigger IDS alerts (like EICAR for antivirus).

```
tiago-paquete@Linux:~$ sudo cat /var/log/suricata/fast.log
==========================================================================
05/06/2025-10:46:33.802418  [**] [1:2100498:7] GPL ATTACK_RESPONSE id
check returned root [**] [Classification: Potentially Bad Traffic]
[Priority: 2] {TCP} 2600:9000:21c3:9400:0018:30b3:e400:93a1:80 ->
2a00:0020:0045:adab:23e9:cb3e:4f3a:07ea:39430
05/06/2025-10:46:39.494637  [**] [1:2100498:7] GPL ATTACK_RESPONSE id
check returned root [**] [Classification: Potentially Bad Traffic]
[Priority: 2] {TCP} 2600:9000:21c3:4800:0018:30b3:e400:93a1:80 ->
2a00:0020:0045:adab:23e9:cb3e:4f3a:07ea:44108
==========================================================================
```

Summary of Fields:

Part	Example	Meaning
Timestamp	`05/06/2025-10:46:33.802418`	When the alert was logged
Generator/ Signature/Revision	`[1:2100498:7]`	Rule info that triggered the alert
Message	`GPL ATTACK_RESPONSE id check returned root`	Description of suspicious activity
Classification	`Potentially Bad Traffic`	Type of alert
Priority	2	Severity level (1 = highest)
Protocol	`{TCP}`	Network protocol used
Source → Destination	`IP:port -> IP:port`	Who sent the packet and who received it

Description of Fields:

1. Timestamp

05/06/2025-10:46:33.802418
Format: MM/DD/YYYY-HH:MM:SS.microseconds

Meaning: The date and precise time the alert was triggered.
Example: May 6th, 2025, at 10:46:33 and 802418 microseconds.

2. Separator

[**]
Just a **visual separator** in Suricata's fast.log format.
Used to make alerts easier to read.

3. Signature IDs

[1:2100498:7]

This identifies **which rule** triggered the alert.
Structure: [Generator-ID:Signature-ID:Revision]

Field	Meaning
1	**Generator ID**: "1" means it's a rule-based alert (from Suricata rules).
2100498	**Signature ID (SID)**: Unique rule ID from the ruleset.
7	**Revision number**: This is the 7th version of that rule.

You can look up SID 2100498 in the Emerging Threats / GPL rule files.

4. Rule Message

GPL ATTACK_RESPONSE id check returned root

Human-readable description of what triggered the rule.
In this case, it's a known attack response pattern indicating someone might have run id and seen uid=0(root) — usually a sign of root access.

GPL = from the **GPL (General Public License)** ruleset, such as Emerging Threats.

5. Second Separator

[**]

Again, just formatting for better readability.

6. Classification

[Classification: Potentially Bad Traffic]

This is defined in Suricata's classification.config.
Category or type of threat this alert belongs to.
Helps group alerts for analysis or dashboarding.

7. Priority

[Priority: 2]

Indicates **severity** or importance of the alert.

Priority	Meaning
1	High severity (likely real attack)
2	Medium severity (suspicious or dangerous behavior)
3	Low severity (informational or policy alerts)

Here, **2 = medium**, meaning it's worth investigating.

8. Protocol

{TCP}

Shows the **transport protocol** involved in the packet.
In this case, TCP (Transmission Control Protocol).

9. Source and Destination

2600:9000:21c3:9400:0018:30b3:e400:93a1:80 ->
2a00:0020:0045:adab:23e9:cb3e:4f3a:07ea:39430

Source:

2600:9000:21c3:9400:0018:30b3:e400:93a1:80

Source IPv6 address and port.

Here:
2600:9000:... is the **source IP**
:80 is the **source port** (HTTP)

Destination:

2a00:0020:0045:adab:23e9:cb3e:4f3a:07ea:39430

Destination IPv6 address and port

:39430 is likely a **random high port** on your machine.