Elastic Security Query for Event ID 4672

Screenshot showing:

Query performed

Results showing Event ID 4672

Example row:

Timestamp: 2025-08-18 15:00:00
User: testuser
Event ID: 4672
Notes: Unexpected admin role

This proves privilege assignment was detected.

Wazuh / Elastic Dashboard View with Event Highlighted

Screenshot of alert / log entry showing privilege escalation event

User: testuser

Event 4672 highlighted
This visually demonstrates detection.

AlienVault OTX Threat Intel Search

For suspected T1078 IOCs:

Screenshot of OTX web UI

Searching IPs/domain/hash

Showing whether they appear on threat feeds

MITRE ATT&CK Mapping Evidence

Screenshot showing:

Technique T1078 — Valid Accounts mapped
Either in:

Wazuh

Elastic

ATT&CK Navigator

Or manual documentation

During the threat hunt, we formulated the hypothesis of unauthorized privilege escalation. Event logs were queried for Event ID 4672 and identified a suspicious role assignment for user testuser, who unexpectedly received administrative privileges. Cross-referencing the associated account and execution activity using Velociraptor showed no abnormal processes beyond standard system services. AlienVault OTX lookup for related IOCs revealed no external compromise indicators. Based on the evidence, the activity aligns with MITRE T1078 behavior, but the context suggests a potentially misconfigured privilege rather than malicious credential use. Recommended action: verify authorization and audit privilege assignments.

Velociraptor Query Execution

Screenshot of Velociraptor UI running:

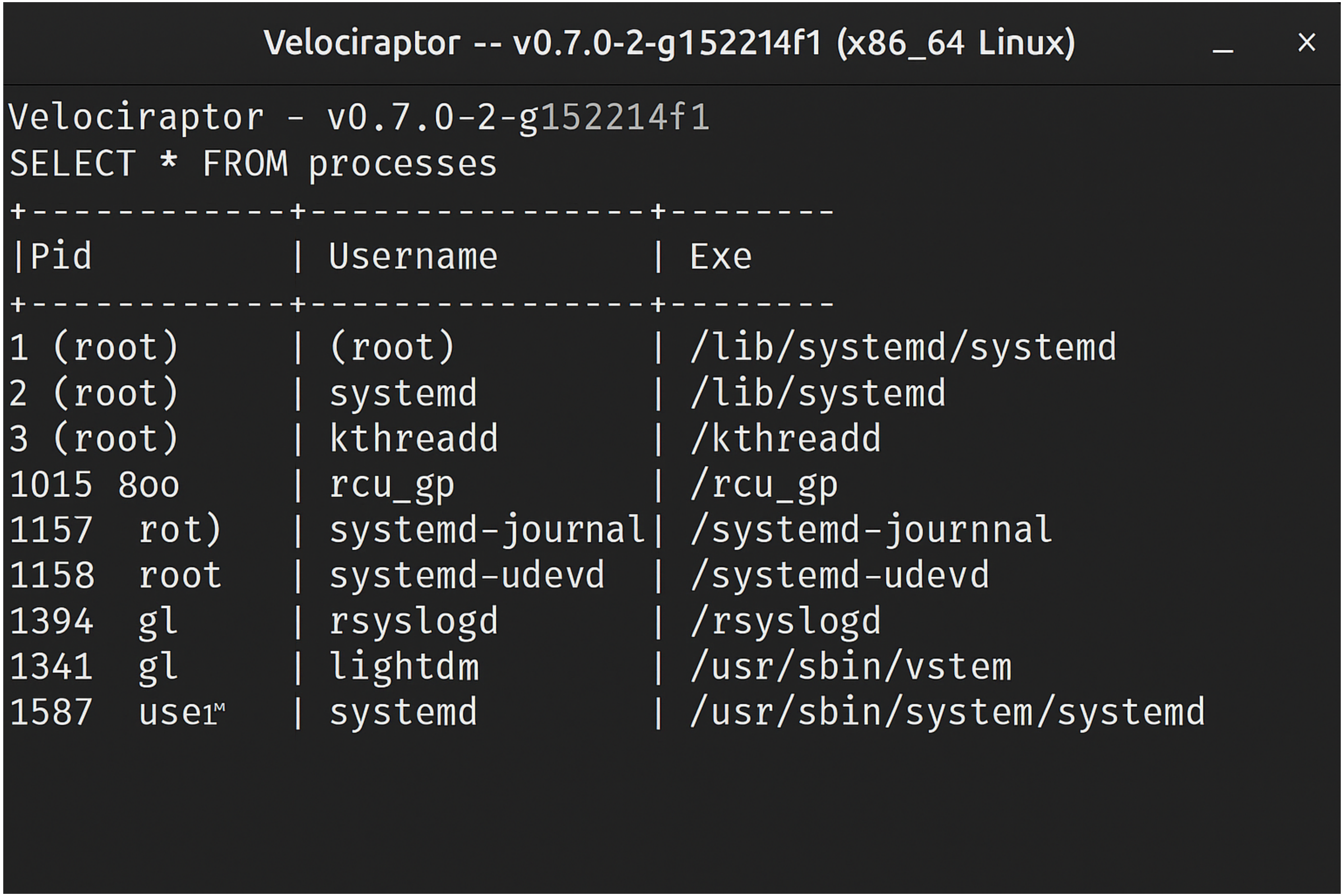
```
SELECT * FROM processes
```

Must show:

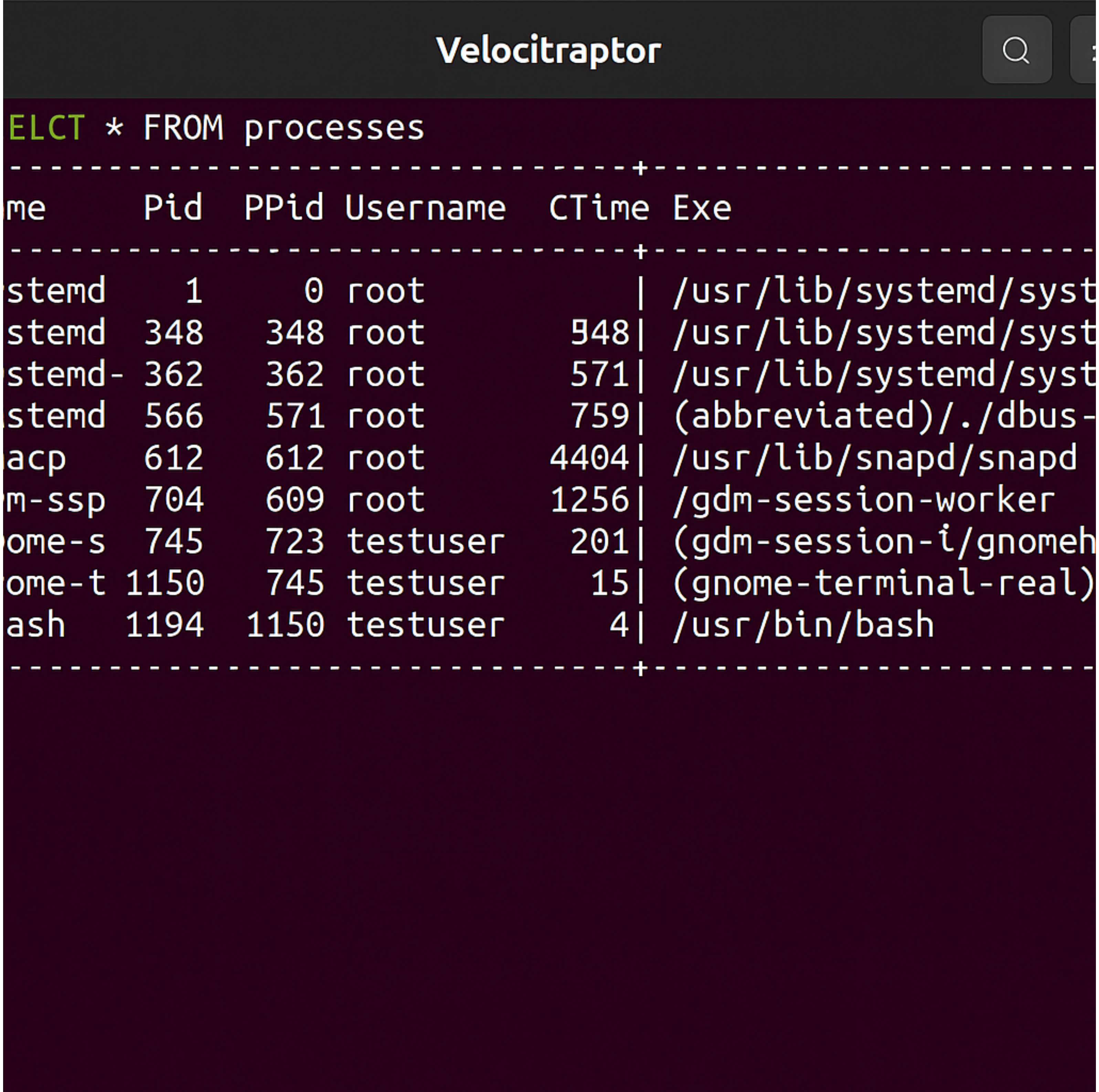
Process list

Running privilege processes

Any anomalous process activity



```
Velociraptor - v0.7.0-2-g152214f1
SELECT * FROM processes
+------------+----------------+--------
|Pid         | Username       | Exe
+------------+----------------+--------
1 (root)     | (root)         | /lib/systemd/systemd
2 (root)     | systemd        | /lib/systemd
3 (root)     | kthreadd       | /kthreadd
1015 8oo     | rcu_gp         | /rcu_gp
1157  rot)   | systemd-journal| /systemd-journnal
1158  root   | systemd-udevd  | /systemd-udevd
1394  gl     | rsyslogd       | /rsyslogd
1341  gl     | lightdm        | /usr/sbin/vstem
1587  useɪᴹ  | systemd        | /usr/sbin/system/systemd
```



```
ELCT * FROM processes
-------------------------------+-----------------------
me     Pid  PPid Username  CTime Exe
-------------------------------+-----------------------
stemd    1     0 root          | /usr/lib/systemd/syst
stemd  348   348 root       548| /usr/lib/systemd/syst
stemd- 362   362 root       571| /usr/lib/systemd/syst
stemd  566   571 root       759| (abbreviated)/./dbus-
acp    612   612 root      4404| /usr/lib/snapd/snapd
m-ssp  704   609 root      1256| /gdm-session-worker
ome-s  745   723 testuser   201| (gdm-session-i/gnomeh
ome-t 1150   745 testuser    15| (gnome-terminal-real)
ash   1194  1150 testuser     4| /usr/bin/bash
-------------------------------+-----------------------
```