Time-Cube Profiling – Venom Scheduler Security Model

1. Alapgondolat

A Time-Cube Profiling egy **belső, időalapú forgalmi önvédelmi modell**, amely nem külső eseményekre, nem triggerekre és nem tartalomelemzésre épül, hanem a rendszer *saját működéséből származó időreferenciákra*.

A cél nem a támadás felismerése, hanem a **rendszer terhelhetőségének és integritásának megőrzése** úgy, hogy a támadó számára a működés teljes egészében **fekete doboz** maradjon.

---

2. Mi az az „idő-kocka” (Time Cube)?

Az idő-kocka egy **belső időszegmens**, amely egy konkrét modul vagy modulcsoport *normál működési idejéből* származik.

Nem: - wall-clock idő - külső időbélyeg - watchdog - trigger

Hanem:

> „Ennek a modulnak ebben a rendszerben **nagyjából ennyi ideig kell futnia**.”

Ez az idő: - determinisztikus - rendszer-specifikus - kívülről nem rekonstruálható

---

3. Miért alkalmas erre a Debian hardening modul-lánc?

A 25 hardening modul: - különböző IO-terhelést okoz - eltérő kernel- és filesystem-interakciókat végez - természetes sorrendben fut

Ez **időprofil-láncot** hoz létre, amely: - nem mesterséges - nem security-logika - hanem a rendszer valódi működése

Ez ideális belső referenciává teszi.

---

4. Mit mérünk egy idő-kockán belül?

A scheduler **nem payloadot elemez**, csak metaadatokat.

Tipikus mért értékek: - beérkező események száma - scheduler queue aktivitás - scheduler aktív idő - feldolgozott események aránya

Kulcsmutató:

> **adatmennyiség / modul-idő arány**

---

5. Normal vs High profil

Normal profil

- várt időtartomány modulonként
- várt eseménysűrűség
- természetes burst + idle minták

High profil

Nem riasztás, hanem **üzemmódváltás**.

Jellemzői: - szűkebb toleranciasáv - konzervatívabb scheduler routing - fokozott NULL Scheduler irányítás

High profilból nincs automatikus visszatérés.

---

6. Slow burn elleni védelem

A modell nem sebességet figyel, hanem: - **időben integrált terhelést** - tartós jelenlétet - profilhoz nem illeszkedő folyamatosságot

Ez ellen a lassítás nem hatásos, mert: - a hatás összeadódik - a rendszer állapota változik

---

7. NULL Scheduler szerepe

A NULL Scheduler: - nem büntet - nem riaszt - nem blokkol

Hanem:

> **elnyel**

Oda kerül minden, ami: - nem illeszkedik az aktuális profilba - nem kritikus - aránytalan terhelést okoz

Ez analóg a `/dev/null` rendszerelvvel.

---

8. Security előnyök

- nincs trigger → nem túlterhelhető
- nincs szabály → nem tanulható
- belső idő → nem megfigyelhető
- fokozatos terelés → nem detektálható

A támadó nem lát: - határértéket - állapotváltást - döntési pontot

Csak azt érzékeli:

> „egyre kevesebb hatása van”

---

9. Alapelv összefoglalás

Ez a modell: - nem IDS - nem SIEM - nem firewall

Hanem:

> **rendszerimmunológia idődimenzióval**

A védelem nem a támadás felismerésén, hanem a **rendszer saját fiziológiáján** alapul.

---

10. Mérnöki minimumelv

> Minél egyszerűbb a mechanizmus, annál nehezebb megtámadni.

A Time-Cube Profiling ezt az elvet követi következetesen.