Tjedan 24.3. - 28.3.

#seminar2

Obrađene usporedbe između alata Suticata, Snort i Zeek
https://sansorg.egnyte.com/dl/l1u6Zjhdgy

[!NOTE] Zaključak rada *"Evaluating the Efficacy of Network Forensic Tools: A Comparative Analysis of Snort, Suricata, and Zeek in Addressing Cyber Vulnerabilities"*

> In 2022, the most exploited vulnerabilities identified by CISA all exhibited network-based exploit signatures detectable by NIDS solutions like Suricata, Zeek, and Snort. The availability of default rules in Snort and Suricata, designed to identify these vulnerabilities, enables cybersecurity teams to focus more on fine-tuning these systems rather than developing new signatures. Leveraging the strengths of each IDS tool is essential for a comprehensive defense strategy. Suricata, Zeek, and Snort each offer distinct functionalities, with Zeek particularly adept at anomaly detection. Employing all three solutions allows organizations to establish a more resilient and adaptable cybersecurity infrastructure, proficient in identifying known vulnerabilities and detecting anomalous behaviors indicative of emerging threats.

Natuknice po poglavljima iz rada:

Snort

- IDS (Intrusion Detection System) s mogućnostima IPS-a.
- Pravila zasnovana na prepoznavanju uzoraka.
- Lagana arhitektura, ali može biti ograničen kod velikih mreža.
  Suricata
- Napredni **IDS/IPS** alat.
- Paralelna obrada paketa → bolja izvedba od Snorta.
- Podrška za multi-threading i GPU akceleraciju.
  Zeek (bivši Bro)
- Fokus na **detaljnoj analizi prometa** umjesto detekcije prijetnji putem pravila.
- Pogodan za dubinsku inspekciju mreže i zapisivanje podataka.

Metodologija evaluacije

- Testiranje provedeno na simuliranom mrežnom okruženju.
- Kriteriji procjene:
  - **Točnost detekcije** (broj ispravnih pozitivnih i lažno pozitivnih slučajeva).
  - **Performanse** (brzina obrade prometa).
  - **Resursna potrošnja** (CPU, memorija).

Rezultati i analiza

Točnost detekcije

- **Suricata** pokazala najbolje rezultate u prepoznavanju prijetnji.
- **Snort** je imao nešto više lažno pozitivnih detekcija.
- **Zeek** nije dizajniran za detekciju napada, ali je dao detaljne zapise.

Performanse

- **Zeek** je imao najmanji utjecaj na performanse sustava.
- **Suricata** je najbrža zbog paralelne obrade.
- **Snort** je imao najveće kašnjenje u analizi prometa.

Resursna potrošnja

- **Zeek** je koristio najmanje CPU resursa.
- **Suricata** je zahtijevala više resursa, ali pružila bolje rezultate.
- **Snort** je imao umjerenu potrošnju, ali slabije performanse.

/	Točnost detekcije	Performanse	Resursna potrošnja
Zeek	3	2	1
Suricata	1	1	3
Snort	2	3	2

Prosječne ocjene (što manje to bolje):

Alat	Prosječna ocjena
Zeek	2

Alat	Prosječna ocjena
Suricata	1.67
Snort	2.33

Zaključak

- **Suricata** je najpogodnija za sustave koji trebaju brzu i točnu detekciju prijetnji.
- **Snort** je dobra opcija za manje mreže s ograničenim resursima.
- **Zeek** je izvrstan alat za forenzičku analizu, ali ne i za detekciju prijetnji u stvarnom vremenu.