Wykrywanie ataków sieciowych - lab 8

Created	@April 27, 2022 11:08 PM
Class	WAS

Zadanie 1

	Snort 2.9	Snort 3.0	Suricata
Wątki pakietów	Jeden na proces	Dowolna liczba na proces (niestabilna funkcja)	Dowolna liczba na proces
Rozruch	Jednowątkowy, wolny	Wielowątkowy, szybki	Wielowątkowy, szybki
Domyślna konfiguracja	Skomplikowana	Uproszczona	Uproszczona
Przyspieszenie sprzętowe	-	-	Wbudowane
Logowanie	Tylko pakiety	Tylko pakiety	Pakiety, certyfikaty TLS/SSL, zapytania HTTP, zapytania DNS
Ekstrakcja plików	-	-	Tak

Zadanie 2

```
alert tcp any any -> any any (msg:"Counting packets with size 1234 and content abcd";
 dsize:1234; content:"abcd"; flowint: packetcount, +, 1; flowbits: noalert;)

alert tcp any any -> any any (msg:"At least 3 packets with size 1234 and content abc
d"; dsize:1234; content:"abcd"; flowint: packetcount, +, 1; flowint:packetcount, >=,
 3;)
```

Zadanie 3

Da się napisać taką regułę z wykorzystaniem słowa kluczowego threshold:

```
alert tcp any any -> any any (msg:"Counting packets with size 1234 and content abcd";
 dsize:1234; content:"abcd"; flowint: packetcount, +, 1; flowbits: noalert;)

alert tcp any any -> any any (msg:"At least 3 packets with size 1234 and content abc
d"; dsize:1234; content:"abcd"; flowint: packetcount, +, 1; flowint:packetcount, >=,
 3; threshold: type limit, track by_src, seconds 600, count 1;)
```

Zadanie 4

```
alert tcp any any -> any any (msg:"Checking login attemp"; content:"user:"; flowbits:
 set, userlogin; flowbits: noalert;)

alert tcp any any -> any any (msg:"Login attemp"; content:"pass:"; flowbits: isset, us
erlogin;)
```