Härtung Suricata [SQL-Injection]

- SQL Injection über Kali ans Host-Netzwerk über die Firewall auf den Webserver
- Nutzung von SQLmap

Alerts für SQL-Injection

```
# Kritisch weil gibt schnellen Alarm wenn jemand irgendwas mit select schreibt
alert http any any -> any any (msg: "SQL-Injection erkannt! (content: Select)"; content:"Select"; nocase;
sid:1000004;)
# Leicht umgehbar weil userAgent geändert werden kann
alert http any any -> any any (msg: "SQLmap erkannt! (user_agent: sqlmap)"; http.user_agent;
content:"sqlmap"; nocase; sid:1000005;)
```

Weitere Möglichkeiten:

- Kommentare "--" im Content suchen (auch kritisch weil schneller Alarm)

Revision #6
Created 6 September 2024 06:57:48 by Max
Updated 6 September 2024 09:16:22 by Max