**Pitanja:**

**Koji je najčešće upozorenje (alert) koji Snort može da detektuje u TCP saobraćaju?**

Neke od najčešćih upozorenja su detekcija aplikacija, pristup zabranjenim resursima, pokušaj korišćenja propusta, slanje/primanje nedozvoljenih datoteka, spam poruke, DoS napadi, itd…

**Koliko različitih DOS napada može Snort naći? Koji su to napadi?**

Snort u default bazi sadrži 16 pravila protiv DoS napada. Neka od njih su: Jolt attack, Teardrop attack, UDP echo+chargen bomb, IGMP dos attack, ISAKMP invalid identification payload attempt, …