1. Koji je najčešće upozorenje (alert) koji Snort može da detektuje u TCP saobraćaju? TCP SYN Flood

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

● DoS based on volume(DoS) .

● DoS attack based on the protocol(DoS)

. ● UDP attack.

● ICMP attack.

● Slowloris Amplification of NTP.

3. Dodati tri nova pravila za Snort.

● alert tcp 192.168.1.0/24 any -> 131.171.127.1 25 (content: “hacking”; msg: ”malicious packet”; sid:2000001;)

● alert tcp any any -> 192.168.1.5 443 (msg:”TCP SYN Flood”; flags:!A; flow: stateless; detection\_filter: track by\_dst, count 70, seconds 10; sid:2000003;)

● alert icmp any any -> $HOME\_NET any (msg: “Ping detected”; sid:1000001; rev:1; classtype:icmp-event;