A black background with red text

Description automatically generated

***IT381 Zaštita i bezbednost informacija***

***Domaći zadatak br. 9***

***Ime i prezime: Jovan Pavkovic***

***Broj indeksa: 4442***

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

Snort je popularan sistem za detekciju intruzija (IDS) koji analizira mrežni saobraćaj i može generisati upozorenja (alerte) na osnovu identifikacije određenih potencijalno zlonamernih aktivnosti. Kada je reč o TCP saobraćaju, jedan od najčešćih upozorenja koje Snort može detektovati je:

Upozorenje na SQL injection (SQLi):

**Opis**: SQL injection je tehnika napada gde napadač pokušava ubaciti zlonamerni SQL kod u upit koji se izvršava na serveru baze podataka. Ovo može dovesti do otkrivanja ili manipulacije podataka u bazi podataka.

**Primer pravila (rule)**:

alert tcp $EXTERNAL\_NET any -> $SQL\_SERVERS $HTTP\_PORTS (msg:"SQL Injection Attack Detected"; flow:to\_server,established; content:"'"; nocase; pcre:"/\b(union|select|insert|update|delete|truncate|drop|alter)\b/i"; sid:XXXXX;)

Ovaj primer pravila ukazuje na detekciju SQL injection napada na osnovu prisustva ključnih reči (npr. "union", "select", "insert", itd.) u TCP saobraćaju upućenom prema SQL serverima.

Pravila se mogu prilagoditi i proširivati u skladu sa specifičnim potrebama organizacije i okoline.

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

Snort (Sistem za detekciju intruzija - IDS) je moćan alat, ali važno je napomenuti da je Snort pasivan sistem detekcije, a ne preventivni sistem. To znači da Snort može detektovati određene vrste napada, uključujući DOS (Denial of Service) napade, ali ne može ih sprečiti. Evo nekoliko vrsta DOS napada koje Snort može detektovati:

* **UDP Flooding:** UDP flood napad podrazumeva slanje velikog broja UDP paketa prema ciljanoj mreži, sa ciljem preopterećenja resursa i ometanja normalnog saobraćaja.
* **SYN/ACK Flooding (TCP SYN/ACK Flood):** Ovaj napad uključuje slanje velikog broja TCP SYN ili ACK paketa prema ciljnom serveru, sa namerom preopterećenja resursa.
* **ICMP Flood:** ICMP flood napad podrazumeva slanje velikog broja ICMP paketa prema ciljnom sistemu, što može izazvati preopterećenje mrežnih resursa.
* **DNS Amplification Attack:** Ova vrsta napada uključuje zloupotrebu DNS servera za generisanje velikog odgovora na malu DNS zahtevnu poruku, što može izazvati preopterećenje ciljanog sistema.

Ovo su samo primeri pravila i vrsta napada. Konkretna podešavanja i pravila zavise od specifičnih potreba organizacije i ciljeva detekcije. Pravilna konfiguracija Snort-a uključuje odgovarajuće podešavanje praga (threshold), praćenje po izvoru (track by\_src), i slično, u skladu sa specifičnostima mreže i pretnji.

* 1. **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;)