A black background with red text

Description automatically generated

***IT381 Zaštita i bezbednost informacija***

***Domaći zadatak br. 11***

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

***Broj indeksa: 4442***

**Tekst zadataka**

1. Preuzeti i instalirati iptables aplikaciju na Linux OS.
   1. Preuzeti dokumentaciju za iptables.
   2. Odgovoriti na sledeća pitanja:
      * Koja komanda briše sva pravila zaštitnog zida?
      * Koja je razlika između FORWARD i OUTPUT lanaca?
      * Objasbiti razlika u korišćenju “-I” i “-A” zastavica (engl. flags) kod konfiguracije iptables
      * Objasniti sledeća iptables pravila:
        + iptables -A INPUT -s ! 161.53.71.0/255.255.255.0 -i eth0 -p udp -m udp

* iptables -A INPUT -s 161.53.2.70 -p udp -m udp --dport 123 -j ACCEPT
* iptables -A INPUT -s ! 161.53.71.235 -i eth0 -p tcp -m tcp --dport 873 -j

DROP

* + - * iptables -A INPUT -i ppp0 -m state -- state NEW,INVALID -j DROP
      * iptables -A FORWARD -i ppp0 -m state -- state NEW,INVALID -j DROP
  1. Napisati sledeća Iptables pravila:
     + Pravilo treba da odbaci bilo koje dolazeće pakete sa IP adrese 192.168.10.35. Host će odgovoriti sa porukom da paket nije prihvaćen zbog REJECT akcije.
     + Pravilo odbacuje sve dolazeće pakete sa IP adrese 192.168.10.35 koji koriste port 23 (telnet).
     + Pravilo dozvoljava zaštitnom zidu da prihvati TCP pakete za rutiranje kada dolaze na interfejs eth0 sa bilo koje IP adrese i šalju se na IP adresu 192.168.1.58 preko interfejsa eth1.
     + Ovo pravilo dozvoljava zaštitnom zidu da pošalje ICMP echo-requests (pings) i da prihvatiCMP koje očekuje.

**Rešenje zadataka**

* Koja komanda briše sva pravila zaštitnog zida? sudo /sbin/iptables -F
* Koja je razlika između FORWARD i OUTPUT lanaca? FORWARD se koristi za pakete koji prolaze kroz uređaj.

OUTPUT se koristi za pakete koji su lokalno generisani, a koji će biti poslati van uređaja.

* Objasbiti razlika u korišćenju “-I” i “-A” zastavica (engl. flags) kod konfiguracije iptables.

-I (insert): pomaže pri ubacivanju jednog ili više pravila u izabranom ili trenutnom lancu.

-A (append): pomaže pri dodavanju jednog ili više pravila na kraj izabranog ili trenutnog lanca.

* Objasniti sledeća iptables pravila:
  + iptables -A INPUT -s ! 161.53.71.0/255.255.255.0 -i eth0 -p udp -m udp --dport 135:139 -j DROP

Svi paketi se poništavaju ukoliko su namenjeni eth0 i protokol je tipa udp i dolaze iz podmreže 161.53.71.0/255.255.255.0

* + iptables -A INPUT -s 161.53.2.70 -p udp -m udp --dport 123 -j ACCEPT Prihvata sve pakete sa adrese 161.53.2.70
  + iptables -A INPUT -s ! 161.53.71.235 -i eth0 -p tcp -m tcp --dport 873 -j DROP Uklanja sve pakete osim onih koji dolaze sa adrese 161.53.71.235 gde je protokol TCP, a port je 873
  + iptables -A INPUT -i ppp0 -m state -- state NEW,INVALID -j DROP

Dodaje se pravilo da se uklone svi paketi koji ne zadovoljavaju set pravila definisan INPUT-om.

* iptables -A FORWARD -i ppp0 -m state -- state NEW,INVALID -j DROP Dodaj pravilo da se dropuju svi paketi koji prolaze kroz uređaj
* Pravilo treba da odbaci bilo koje dolazeće pakete sa IP adrese 192.168.10.35. Host će odgovoriti sa porukom da paket nije prihvaćen zbog REJECT akcije. iptables -A INPUT -s 192.168.10.35 -j REJECT
* Pravilo odbacuje sve dolazeće pakete sa IP adrese 192.168.10.35 koji koriste port 23 (telnet).

iptables -A INPUT -s 192.168.10.35 -p tcp –dport 23 -j REJECT

* Pravilo dozvoljava zaštitnom zidu da prihvati TCP pakete za rutiranje kada dolaze na interfejs eth0 sa bilo koje IP adrese i šalju se na IP adresu 192.168.1.58 preko interfejsa eth1.

Iptables -A PREROUTING -t nat -i eth0 -p tcp –dport -j DNAT –to 192.168.1.58:80 Iptables -t nat -A POSTROUTING -d 192.168.1.58 -p tcp –dport 80 -j

MASQUERADE

Ovo pravilo dozvoljava zaštitnom zidu da pošalje ICMP echo-requests (pings) i da prihvatiCMP koje očekuje.

Iptables -D OUTPUT -p icmp –icmp-type echo-reply -j DROP