

### Pitanje 1

Nije još odgovoreno

Broj bodova od 3,00

Proučite manual za naredbu iptables: `man iptables`. Koja je razlika između INPUT, OUTPUT i FORWARD lanaca kod filtriranja paketa?

Iptables koristimo za filtriranje paketa u kernelu.

INPUT se odnosi na sve dolazne pakete čija je primjena lokalni sustav, preko njega se filtriraju paketi prije nego što dođu do lokalnih aplikacija

OUTPUT filtrira odlazne pakete prije nego što stignu do mreže iz lokalnog sustava

FORWARD se koristi za pakete koji prolaze kroz lokalni sustav ali tamo ne koriste.

Blokiranje određenih IP adresa ili samo dopuštanje određenih vrsta su svojstva koja sadrže navedeni lanci.

### Pitanje 2

Nije još odgovoreno

Broj bodova od 3,00

Koja je razlika između skeniranja tipa TCP SYN scan i TCP connect scan? S kojim zastavicama je potrebno pozvati nmap za skeniranje TCP SYN, a s kojim zastavicama za skeniranje TCP connect tipom?

TCP SYN i TCP connect scan su 2 različita načina skeniranja gdje je TCP SYN brz, diskretan i koristimo ga u skeniranjima portova.

TCP connect scan je manje diskretan jer uspostavlja potpunu vezu i zbog toga ga je puno lakše otkriti. Koristi 3-way rukovanje da ustanovi status porta na odredišnom računalu gdje TCP SYN to radi preko zastavice (ako primi SYN/ACK onda je otvoren, ako dobije RST zatvoren)

Zastavice

TCP SYN = `-sS` u nmapu --> `nmap -sS odredisna-ip`

TCP connect scan = `-sT` --> `nmap -sT odredisna-ip`

### Pitanje 3

Nije još odgovoreno

Broj bodova od 3,00

Proučite *manual* za konfiguraciju SSH poslužitelja `sshd_config`: *man sshd\_config*.

Nalazi se na putanji `/etc/ssh/sshd_config`.

- `port` = postavlja TCP port, standardni 22
- `PermitRootLogin` = prijava kao root
- `PasswordAuthentication` = korištenje lozinke za autentifikaciju
- `AllowUsers` = odabir korisnika koji se mogu prijaviti

### Pitanje 4

Nije još odgovoreno

Broj bodova od 3,00

Istražite "jump host" način pristupa i objasnite zašto bi se uopće takav način koristio za spajanje na SSH poslužitelj.

To je mehanizam pomoću kojeg se korisnik spaja preko jump servera. Koristan je u velikim organizacijama za spajanje više korisnika i servera.

Upotrebljava se jer smanjuje izloženost SSH servera na internetu i mogućnost napada. Nalazi se iza firewalla koji se može podešavati i kontrolirati. Serveri se mogu prijavljivati na Jump host i tako se smanjuje administracija.