Ping flood i zaštita od njega

Ping flood je jedan od načina napada uskraćivanjem usluge (denial-of-service). Napadač šalje što je moguće više "pingova" prema žrtvinom računalu, izazivajući slanje odgovora, što troši procesorske cikluse i opterećuje mrežu. Napad je uspješniji ako napadač ima bržu mrežu nego žrtva, jer može poslati više *ICMP echo* zahtjeva. Napadom s više računala odjednom učinak se multiplicira.

Najjednostavniji način da neko računalo "preplavite" *ICMP echo requestima* je korištenje dobre stare naredbe *ping*, ali s *root* ovlastima i s prekidačem -f, koji znači *flood*.

```
$ sudo ping -f 192.168.1.1
```

Povećane ovlasti nam trebaju jer običan korisnik može slati pingove u razmacima od 200 ms, a nama ovdje treba veća brzina.

Kako se obraniti od ovakvog rasipanja resursa, kada vaš server napadnu ping floodingom?

Najjednostavnije i najbrže rješenje je naprosto odbaciti sve *ICMP echo* zahtjeve, na primjer ovako:

```
# sysctl -w net.ipv4.icmp_echo_ignore_all=1
```

ICMP protokol se zapravo koristi za dijagnostiku rada mreže i ne bi ga trebalo isključivati. Zato ćemo ga, kad napad završi, ponovo uključiti:

```
# sysctl -w net.ipv4.icmp_echo_ignore_all=0
```

Malo obzirniji način zaštite je da usporite slanje odgovora na adresu s koje dolaze pingovi:

```
# sysctl -w net.ipv4.icmp_echoreply_rate=10
```

iptables nude način da se sačuva dijagnostička funkcionalnost, a istovremeno odbaci *ping flooding* napade.

```
# iptables -A INPUT -p icmp -m icmp -m limit --limit 1/second -j ACCEPT
```

Odsada ćemo primati samo jedan *ICMP echo request* u sekundi sa svake pojedinačne IP adrese.

Pinganje koriste i neke aplikacije. Na primjer BackupPC prije nego pristupi računalima s kojih se spremaju podaci pinganjem provjerava da li je računalo na mreži. Blokiranjem *pinga* blokirali bismo i *backup* poslovnih podataka.

Već dugo u praksi nisam doživio *ping flood* napad, no povremeno će ga netko pokušati isprobati, makar iz radoznalosti. Zato ne škodi unaprijed postaviti obranu, zadržavajući pritom normalnu fukncionalnost ICMP protokola.

pet, 2013-07-26 08:54 - Aco Dmitrović**Kuharice:** Linux [1]
Kategorije: Sigurnost [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1298

Links
[1] https://sysportal.carnet.hr/taxonomy/term/17
[2] https://sysportal.carnet.hr/taxonomy/term/30