Kako prepoznati "SYN flooding"


Sigurno ste ponekad primjetili u kernel log datoteci zapise poput ovoga:

```
Feb 12 12:34:27 s1 kernel: possible SYN flooding on port 80.
  Sending cookies.
Feb 12 14:12:40 s1 kernel: possible SYN flooding on port 80.
  Sending cookies.
...
Feb 12 14:14:57 s1 kernel: possible SYN flooding on port 80.
  Sending cookies.
Feb 12 14:18:15 s1 kernel: possible SYN flooding on port 80.
  Sending cookies.
```

Radi se o SYN flooding napadu koji u pravilu nema neki utjecan na dobro konfiguriranu mrežu i poslužitelj. SYN flooding radi na način da poslužitelju pošalje SYN requests koji nikad ne završi sa ACK te na taj način poslužitelj koristi mrežni slot čekajući drugu stranu za odgovor. Šaljući sve više SYN flooding napada mrežni resursi postaju popunjeni, te poslužitelj nakon nekon vremena postaje neupotrebljiv.

Simptomi koji se javljaju sa strane krajnjeg korisnika su sporo i dugo učitavanje web stranice. Moguće je da se učita samo dio stranice.

Problem na koji sistemac može naići je da prilikom SYN flooding napada ne može primjetiti visoku opterećenost CPU-a.

Način na koji možemo primjetiti da se radi o SYN floodin napadu da iskoristimo naredbu time u kombinaciji sa wget i vidjeti koje je vrijeme potrebno za učitavanje.

```
$ time wget -O /dev/null server1.server.hr
--2010-02-12 15:00:02--  http://server1.server.hr/
Resolving server1.server.hr... 192.168.1.1
Connecting to server1.server.hr|192.168.1.1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6601 (6.4K) [text/html]
Saving to: `/dev/null'

100%[==========================>] 6,601   --.-K/s   in 0s

2010-02-12 15:00:02 (233 MB/s) - `/dev/null' saved [6601/6601]

real    0m0.007s
user   0m0.000s
sys    0m0.004s
```

Učitavanje je trajalo svega 7 milisekundi što je u ovom primjeru sasvim normalno.

U usporedbi kad se radi o SYN floodin napadu rezultat je puno drugačiji:

```
$ time wget -O /dev/null server1.server.hr
--2010-02-12 15:00:02--  http://server1.server.hr/
Resolving server1.server.hr... 192.168.1.1
Connecting to server1.server.hr|192.168.1.1|:80... connected.
```

Ovdje vidimo da proces učitavanja nije još završio, poslužitelju treba dosta vremena da otvori mrežnu utičnicu
te moramo pričekati krajnji rezultat.

Nakon podužeg čekanja dobijemo rezultat:

```
HTTP request sent, awaiting response... 200 OK
Length: 6601 (6.4K) [text/html]
Saving to: `/dev/null'
...
real    0m52.008s
...
```

Primjetit ćemo da je potrebno 52 milisekunde za (lokalno) učitavanje.

Pomoću naredbe netstat izvršit ćemo provjeru konekcija na poslužitelj:

```
$ netstat -tuna | grep :80 | grep SYN_RECV
```

Kao rezultat dobijemo hrpu SYN request zahtjeva sa iste IP adrese:

```
tcp        0      0 192.168.1.1:80      x.y.z.y:58260      SYN_RECV
tcp        0      0 192.168.1.1:80      x.y.z.y:58259      SYN_RECV
tcp        0      0 192.168.1.1:80      x.y.z.y:54755      SYN_RECV
tcp        0      0 192.168.1.1:80      x.y.z.y:54753      SYN_RECV
...
tcp        0      0 192.168.1.1:80      x.y.z.y:54756      SYN_RECV
tcp        0      0 192.168.1.1:80      x.y.z.y:54754      SYN_RECV
```

Način na koji se možemo zaštiti je uključivanje SYN cookies na poslužitelju pomoću naredbe sysctl.

```
sysctl -w net.ipv4.tcp_syncookies=1
```

U konfiguracijsku datoteku /etc/sysctl.conf moramo dodati redak:

```
net.ipv4.tcp_syncookies=1
```

kako bi ova funkcija radila i nakon ponovnog startanja poslužitelja. Na CARNetovim poslužiteljima je ovaj redak već dodan, ukoliko rabite paket kernel-2.6-cn.

Zdravko Rašić

- Logirajte [1] se za dodavanje komentara

uto, 2010-02-16 12:38 - Zdravko Rašić**Kuharice:** Linux [2]
Kategorije: Mrežna sigurnost [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/717

Links
[1] https://sysportal.carnet.hr/sysportallogin
[2] https://sysportal.carnet.hr/taxonomy/term/17
[3] https://sysportal.carnet.hr/taxonomy/term/33