

Ochrana proti DDoS za použitia open-source software

Katarína Ďurechová • katarina.durechova@nic.cz • 30.11.2013

Distributed Denial of Service

- odopretie služby
 - dosiahnutím limitu
 - pripojenia
 - sieťovej karty
 - CPU
 - pamäte
 - aplikácie



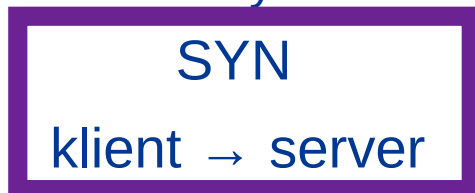
Útoky

- Slowloris
 - stačí jeden počítač, nevyžaduje aby sa posielalo veľa dát
 - posiela čiastočné requesty, potom posiela ďalšiu časť http hlavičky ešte pred timeoutom, takže drží otvorené spojenia
 - pôvodne perlový skript, my používame vlastnú implementáciu v C



Útoky

- Syn flood
 - TCP 3-way handshake



SYNACK

server → klient

ACK

klient → server

- často podvrhnutá zdrojová adresa
 - problém pre CPU
 - 4-jadrové CPU zvláda útoky lepšie ako 1-jadrové



Ochrana

- nginx
- varnish
- parametre kernelu



iptables

- nemusí byť vhodné pri proxy, NAT
- nepomôže s random source-ip syn-floodom



iptables

obmedzenie per requesty:

- `iptables -A INPUT -p tcp --dport 80 -m state --state NEW -m recent --set`
- `iptables -A INPUT -p tcp --dport 80 -m state --state NEW -m recent --update --seconds 1 --hitcount 20 -j DROP`
- `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`

obmedzenie per spojenie:

- `iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 80 -j DROP`
- `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`

25/sec, stav sa dá pozrieť v `/proc/net/iptables_hashlimit/DoS-DNS`:

- `iptables -N dns_udp`
- `iptables -A INPUT -p udp --dport 53 -j dns_udp`
- `iptables -A dns_udp -m hashlimit --hashlimit-above 25/sec \
--hashlimit-burst 100 --hashlimit-mode srcip \
--hashlimit-name DoS-DNS -j DROP`
- `iptables -A dns_udp -j ACCEPT`



Parametre kernelu /etc/sysctl.conf

- SYN cookies
 - zakázanie logovania martian paketov
 - rp_filter
-
- sysctl -p



Limity /etc/security/limits.conf

```
varnish soft memlock 82000  
varnish hard memlock 82000  
varnish soft nofile 100000  
varnish hard nofile 500000
```

```
nginx soft memlock 82000  
nginx hard memlock 82000  
nginx soft nofile 100000  
nginx hard nofile 500000
```



Limity `/etc/security/limits.conf`

- defaultne sú príliš nízke
- zvýšenie maximálneho počtu otvorených file deskriptorov
- zvýšenie adresného priestoru v uzamknutej pamäti
 - pre varnishlog, varnishtop



nginx

- worker_processes 4;
events {
- worker_connections 250000; }
- http {
- ignore_invalid_headers on;
- limit_req_zone \$binary_remote_addr zone=slimits:1m rate=60r/m;
- proxy_connect_timeout 90;
- proxy_send_timeout 90;
- proxy_read_timeout 90;
- proxy_buffer_size 4k;
- proxy_buffers 4 32k;
- proxy_busy_buffers_size 64k;
- proxy_temp_file_write_size 64k;

- server {
- set \$limit_rate 100k;
- client_body_buffer_size 8k;
- client_max_body_size 1k; } }



nginx

- `worker_processes` – podľa počtu jadier
- `worker_connections` – počet spojení per worker
- nastavenie
 - limitov
 - timeoutov
 - bufferov



varnish

- /etc/default/varnish:

```
NFILES=100000
```

```
MEMLOCK=82000
```

```
START=yes
```

```
DAEMON_OPTS="-a :80 -u varnish -g varnish -w 50,1000,60
```

```
-f /etc/varnish/default.vcl -T127.0.0.1:6082
```

```
-S /etc/varnish/secret -s malloc,1G"
```

-a definuje adresu a port na ktorom budeme poslúchať

-w minimálny a maximálny počet vláken workerov, a timeout

-T adresa a port management rozhrania

-s typ a veľkosť storage (pamäť, alebo súbor)



/etc/varnish/default.vcl

aby sme dostali pôvodnú adresu klienta:

```
sub vcl_pipe {
    set bereq.http.connection = "close";
    if (req.http.X-Real-IP) {
        set bereq.http.X-Real-IP = req.http.X-Real-IP;
    } else {
        set bereq.http.X-Real-IP = regsub(client.ip, ".*", "");
    }
}
```

```
sub vcl_pass {
    set bereq.http.connection = "close";
    if (req.http.X-Real-IP) {
        set bereq.http.X-Real-IP = req.http.X-Real-IP;
    } else {
        set bereq.http.X-Real-IP = regsub(client.ip, ".*", "");
    }
}
```



HAProxy – load balancer

- <http://haproxy.1wt.eu/download/1.3/examples/antidos.cfg>
- konfiguračný súbor prispôsobený na odolávanie voči DDoSu



Meranie

- `httpperf --server 192.168.1.3 --num-conn 27000 --rate 500 --timeout 5 --port 80`
- 5 meraní/bunka
- Requesty, ktore sa dostali na server:

	normal	synflood	slowloris	sf+sl
apache2	27000	14289	6580	1163
nginx	27000	19265	23223	19452
nginx+a2	27000	19961	25862	19575
varnish+a2	27000	19793	26476	19644
varnish+nx	27000	20247	26924	18795



BSD firewall pf

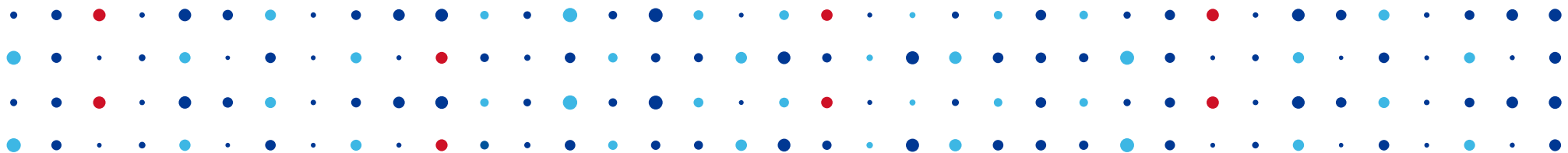
- pass in on \$ext_if proto tcp to \$web_server port www synproxy state
 - spraví s klientom prvotný 3-way handshake
 - aj v iptables 1.4.21 vďaka Patrickovi McHardymu
 - <http://thread.gmane.org/gmane.linux.network/278834>
- antispooof for fxp0 inet
 - sa rozšíri do:
 - block in on ! fxp0 inet from 10.0.0.0/24 to any
 - block in inet from 10.0.0.1 to any



BCP-38 Ingress filtering

- <http://tools.ietf.org/html/bcp38> - RFC
- <http://www.bcp38.info/>
- implementácie:
 - kernel parameter `rp_filter`
 - pf antispoof





Ďakujem za pozornosť

Katarína Ďurechová • katarina.durechova@nic.cz

