# Knocking on Heaven's Door, 1. dio

Poetski naslov ovog članka, kojeg ćemo zbog duljine objaviti u dva dijela, inspiriran je načinom na koji se pokušava riješiti problem napada, najčešće preko SSH protokola. Naime, u zadnje vrijeme je primjećen povećan broj pokušaja upada na poslužitelje preko tog protokola. Iako su uspješni upadi i bez dodatnih zaštita relativno rijetki, ne treba ih nikada u potpunosti zanemariti. Već smo opisali nekoliko metoda zaštite, fail2ban [1]i dali recepte za uporabu ipt_recent [2]modula u iptablesima, no napadači konstantno mijenjanju načine napada i treba ih spremno dočekati.

Sustavi poput fail2bana uspješno zaustavljaju napade koje dolaze s iste adrese, no ne mogu zaustaviti napade koje dolaze s mnogo adresa, i to namjerno usporenim ritmom i korisničkim imenom. U logovima (/var/log/auth.log) to izgleda otprilike ovako:

```
Jan 17 18:34:28 srv sshd[12635]: Failed keyboard-interactive/pam for invalid
user simon from 200.40.XX.6 port 12601 ssh2
Jan 17 18:36:24 srv sshd[12949]: Failed keyboard-interactive/pam for invalid
user sistemas from 113.17.XX.199 port 41059 ssh2
Jan 17 18:36:35 srv sshd[12953]: Failed keyboard-interactive/pam for invalid
user site from 193.62.XX.134 port 44625 ssh2
```

Nadajući se da će proći "ispod radara", napadač ne ponavlja napad s istog računala (nego vjerojatno iz nekog BotNeta [3]), ne napada istog korisnika, niti pokušava pogoditi zaporku previše puta u minuti. Sve ovo čini u nadi kako će izbjeći IDS [4](Intrusion Detection) sustave, što mu, očigledno, može uspjeti.

Naravno, još uvijek valja pogoditi ispravnu kombinaciju korisnika i zaporke, no kad jednom napadači uđu u sustav, sve je daleko lakše. Mnoge ranjivosti, koje inače ne mogu iskoristiti udaljeno, sada su im na dohvat ruke.

Najjednostavnija obrana, barem što se SSH protokola tiče, je promijeniti osnovni port na kojem servis "sluša". Mnogi su to već odavno učinili, no iako to u ovom slučaju može pomoći, nije nikakva zaštita od "pravih" hackera, kojima neće biti nikakav problem prepoznati koji servis sluša na nekom neuobičajenom portu.

Kao vatrogasnu mjeru, dakle, možemo jednostavno promijeniti port na kojem sluša SSH daemon. Što treba promijeniti? Treba promijeniti direktivu "Port" u datoteci /etc/ssh/sshd_config i restartati sshd. Port je proizvoljan (ako nije zauzet), no morate obavijestiti sve korisnike da se port promijenio. Ako nitko osim vas ne rabi SSH, tim bolje - ne morate nikoga obavještavati.

U /etc/ssh/sshd_config upišite:

```
#Port 22
Port 12345
```

Nakon toga, kao što već vjerojatno znate, treba restartati servis:

```
# /etc/init.d/ssh restart
```

Mnogima će i ovakvo rješenje biti zadovoljavajuće, no može se mnogo više.

Ovdje dolazimo otkud nam naslov članka: od pojma "port knocking". Radi se o načinu zaštite (neki bi rekli da je to ipak samo jedan način "security through obscurity [5]"), koji otvara SSH port (zapravo, može i bilo koji drugi) samo pod određenim uvjetima. Ti uvjeti su doslovce "kucanje na portove", odnosno morate se pokušati spojiti na unaprijed predoodređen niz portova unutar vremena, prije nego se otvori port 22.

Na taj način napadač ne može znati da postoji SSH servis, jer port 22 nije otvoren. Ni skeniranjem ostalih portova neće ništa saznati, jer samo određeni niz otvara port 22 (npr. mora se proći niz portova 7777, 1234, 8888, 9876). Dakle, slučajnim skeniranjem se ne može otkriti niz koji otvara port 22 (portove nemojte odabrati u nizu, 7777, 7778, 7779 itd).

Portovi ne moraju biti TCP, nego mogu biti i UDP, što dodatno komplicira napad. Možda najveća sigurnosna prednost je mogućnost da poslani paketi moraju sadržavati točno određene TCP zastavice (SYN, FIN, URG...), inače knock niz neće biti uspješan.

Prednosti Port knockinga se otprilike ovdje, nažalost, završavaju.

Negativne strane Port knockinga su:

- unosi dodatno kašnjenje prilikom spajanja na poslužitelj jer korisnik mora napraviti dodatne predradnje

- moguće je, uz određene tehničke pretpostavke i znanje, presresti sekvencu portova, i na taj način zaobići zaštitu

- morate otvoriti te knock portove na vatrozidu, te je sposobnom hackeru moguće nizom pokušaja doći do prave kombinacije

- ne podržava enkripciju, barem u osnovnoj izvedbi

Postoje druge implementacije Port knockinga, koje pokušavaju umanjiti ove nedostatke, ali u svrhu dodatne zaštite i "obični" knocking je dobar.

Više o Port knockingu pročitajte na http://www.portknocking.org, ili na drugim web sjedištima gdje se objašnjava princip rada.

U sljedećem nastavku ćemo vam pokazati kako upogoniti cijeli sustav i unijeti dodatnu razinu zaštite na vaš poslužitelj.

- Logirajte [6] se za dodavanje komentara

pon, 2010-01-18 12:07 - Željko Borš**Kuharice:** Linux [7]
**Kategorije:** Servisi [8]
**Vote:** 4

Vaša ocjena: Nema Average: 4 (1 vote)

**Source URL:** https://sysportal.carnet.hr/node/698

**Links**
[1] https://sysportal.carnet.hr/node/542
[2] https://sysportal.carnet.hr/node/71
[3] http://en.wikipedia.org/wiki/Botnet
[4] http://en.wikipedia.org/wiki/Intrusion_detection_system
[5] http://en.wikipedia.org/wiki/Security_through_obscurity
[6] https://sysportal.carnet.hr/sysportallogin
[7] https://sysportal.carnet.hr/taxonomy/term/17
[8] https://sysportal.carnet.hr/taxonomy/term/28