

# Port Knocking

Knock knock knockin' Heavens Port...

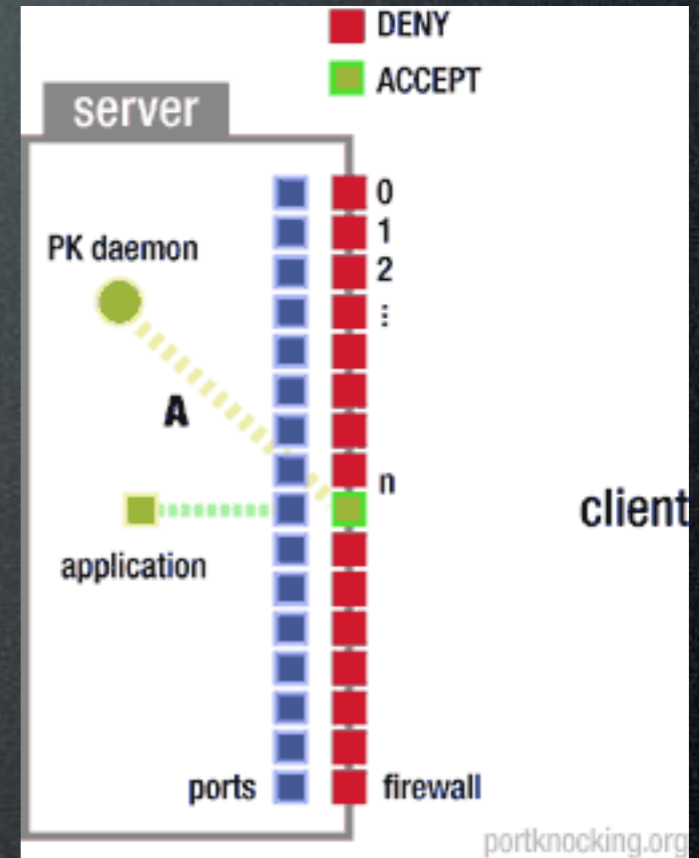
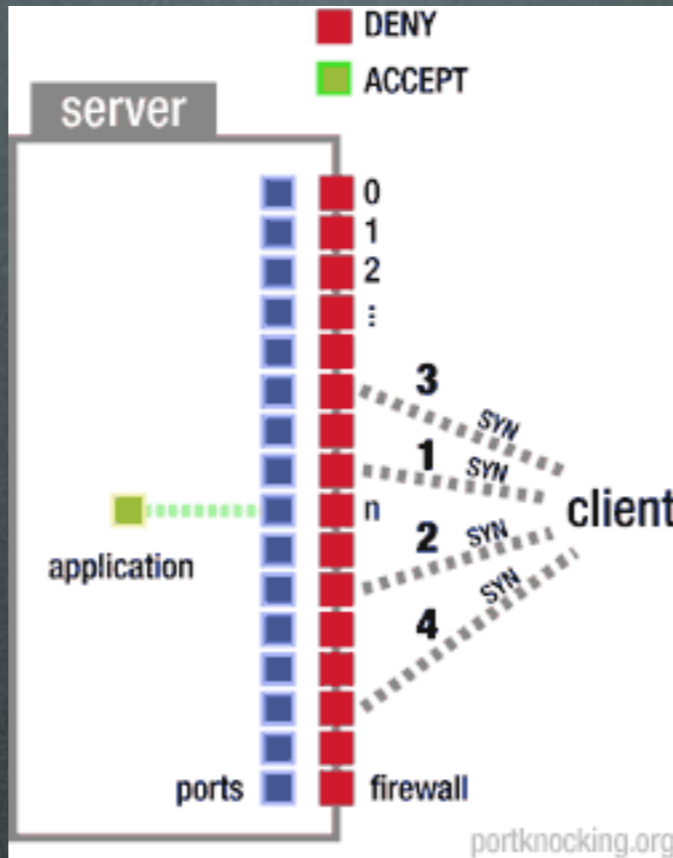
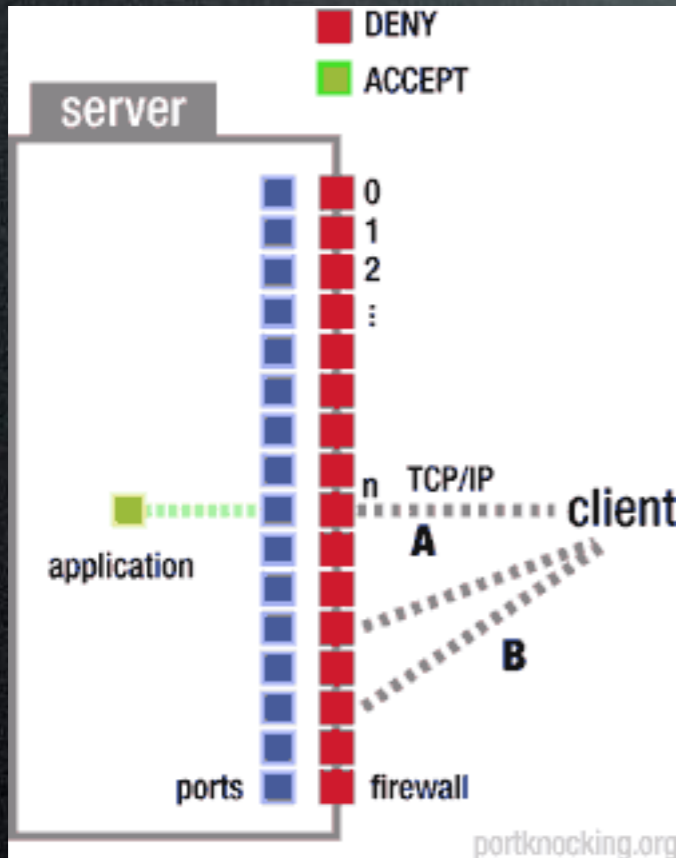
Liudas Sodonis aka @lfx

<http://liudas.sodonis.eu/>

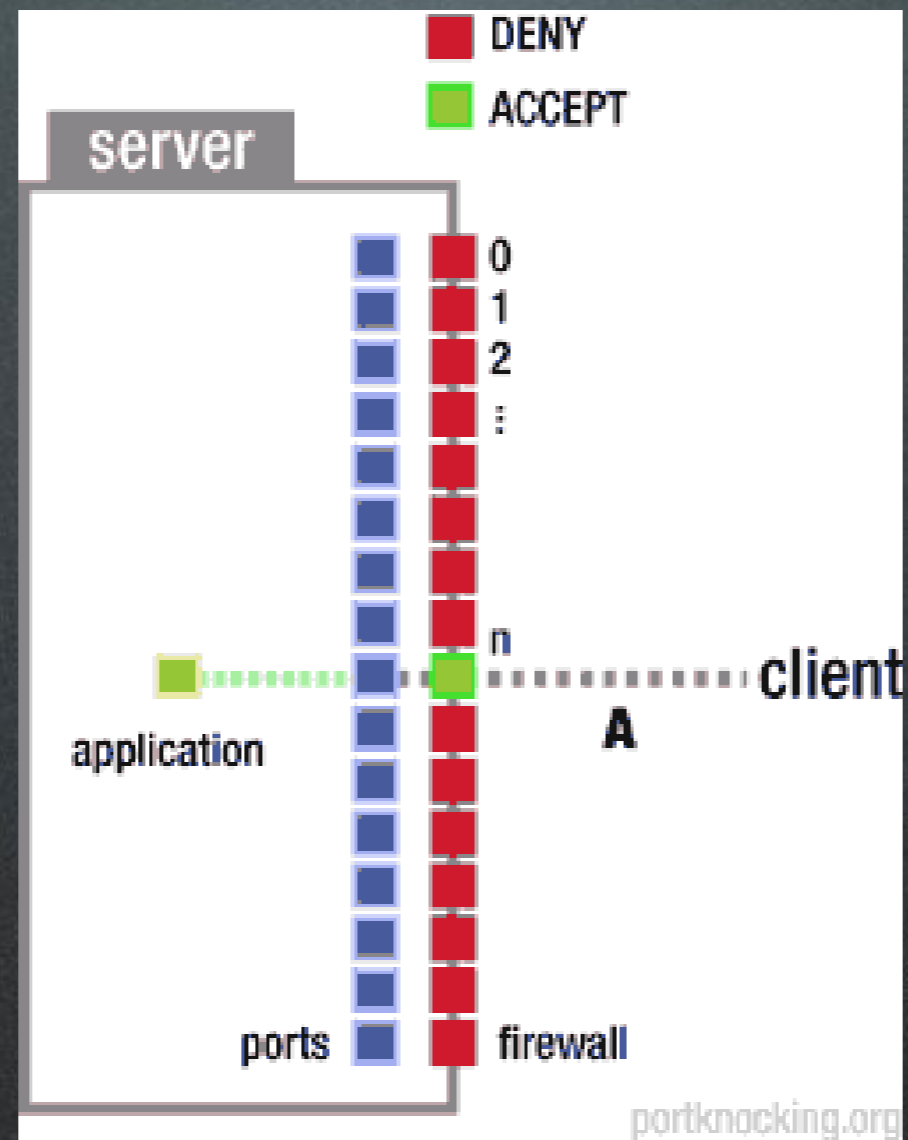


- Tai lyg Morzės abėcėlė.
- Pasibeldžiu, mane suprato kaip draugą atidarė duris, nesuprato - neįvyko nieko.

# Veikimo principas



# Veikimo principas



# Įvairios implementacijos

- Simple
- Advanced
- One Knock
- DNS Knock

# Advanced

102,100,110	10a,10b,10c,10d	$10(a+b+c+d \bmod 10)$	110,100,102
header	payload	checksum	footer

- Portai 100-109
- abcd - portas kurį reikia atidaryti
- Tarkim 143 (checksum  $8 = 1+3+4 \bmod 8$ )
- 102,100,103 100,101,104,103 108 103,100,102
- Via Jennifer C. Hou University of Illinois

# SIMPLE 1 shell

- iptables logina
- scriptas tail -f
- apdoroja
- vykdo

# SIMPLE 1 shell ex:

- show2.txt

# SIMPLE 2 py

- iptables logina
- **knockknock** demonas sukas ir sukas
- <http://www.thoughtcrime.org/software/knockknock/>

# SIMPLE 2 tcpdump

- show3.txt

# Advanced pure iptables

- Iptables sukuriama taisyklės ir grandinės (chain)
- Paketai vaikšto tarp taisyklių
- Atidaromas portas

# Advanced pure iptables ex:

- show1.txt

# One Knock - Doorman

- Senas ir patyręs kaip ir turi būti tikras liokajus.
- Sakos esąs saugus.
- Moda visas kalbas (win,\*nix)
- Moka ne tik atidaryti portus, bet ir atlikti kitus veiksmus
- <http://doorman.sourceforge.net/>

# One Knock - Tariq

- Naujas, Arabiškas, Įdomus
- Py, Crypto, Sniff
- Ne tik atidaro portus, bet vykdo ir kitokias komandas
- Pvz: httpd restart, bot attack visa.com, ir kt.
- <http://code.google.com/p/tariq/>

# Tariq veikimo principas

- Cli – užkoduoja veiksmą į img naudodamasis Stenografija.
- Cli – įdeda į TCP SYN paketa payloadą.
- Srv – pagauna paketą, iškoduoja, randa img, iškoduoja img randa komandą.
- Srv – sugeneruoja rand skaičių, užkoduoja us PGP įmeta į img, išsiunčia atgal pas Cli

# Tariq veikimo principas

- Cli – gauna paketa, išsikoduoja su savo PGP raktu.
- Cli – sugeneruoja su savo public raktu tą patį skaičių, išsiunčia Srv.
- Srv – pagauna, paketa, jį išsikoduoja su savo raktu, sulygina, ar tikrai tas, kurį siuntė. Ir jei taip:
- Srv – atlieką veiksmą, kurį gavo pirmajame pakete.

# DNS knock / Paketai

- Kreipiamės į DNS serverą, klausiam apie xxx.com
- Demonas analizuoja DNS logus ....
- Linux distributyvo paketas **knockd**.

# Pros

- Nėra atvirų jungčių
- Mažai tikėtinas burterforsinimas nes trijų knocku perrinkimas ....
- ~281 trilijonai galimybių
- nix\* praktiškai imi ir paleidi
- Net perėmus srautą šifruotais paketais sudėtinga suprasti kas vyksta.

# Cons

- Nulūš demonas ir liksi be servo (nors protingos sistemos...)
- Perėmus kliento kompa galima sužinot seką ir t.t.
- Reikia uždarų jungčių diapazono.
- Prie apkrauto servo gali būti sunku prisijungti

# Src

- <http://www.portknocking.org>
- [http://en.wikipedia.org/wiki/Port\\_knocking](http://en.wikipedia.org/wiki/Port_knocking)
- Hakin9 2010 05.
- Martin Krzywinski (<http://mkweb.bcgsc.ca>)

