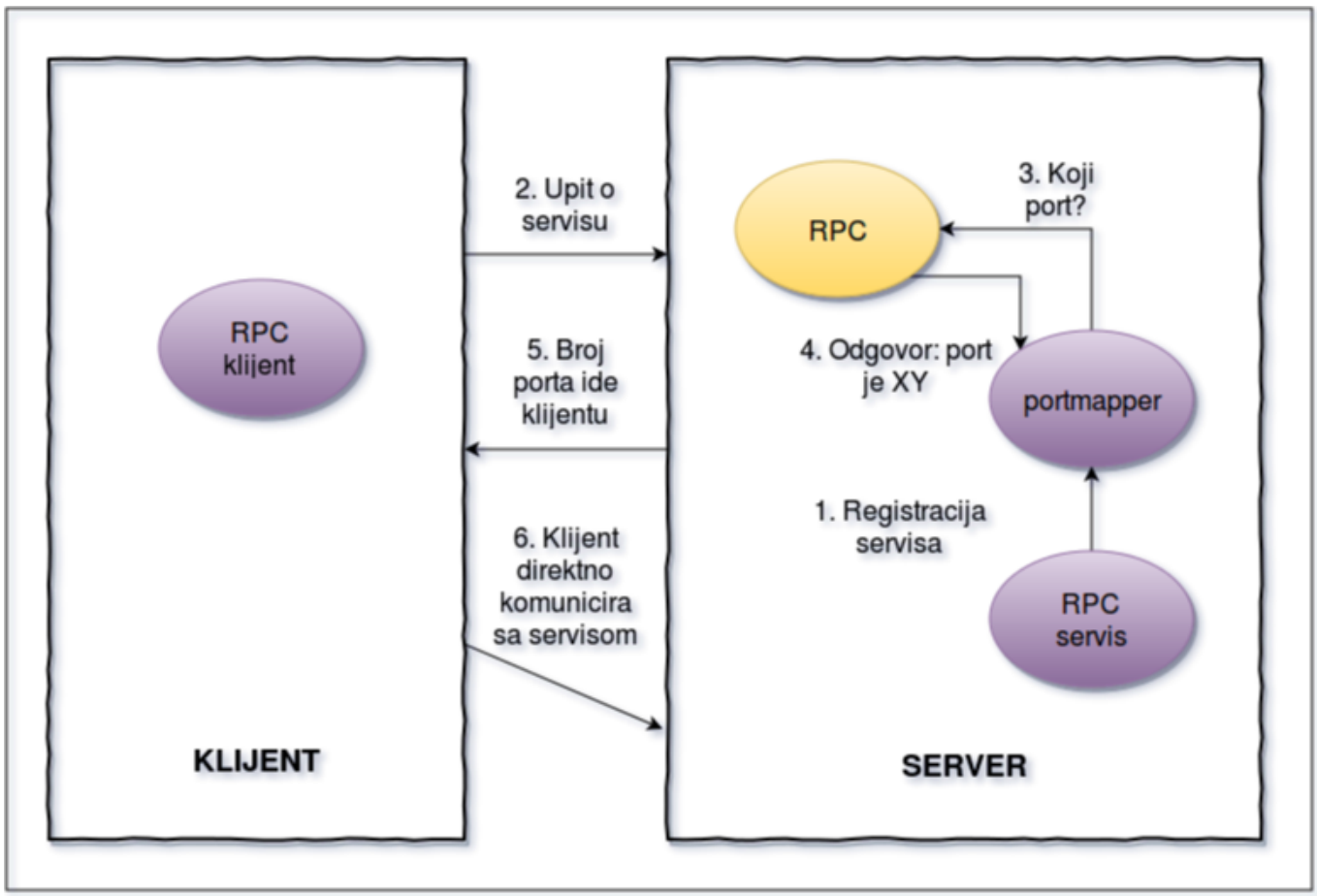
# Kako ograničiti ili onemogućiti rpcbind?

Ukoliko ste ovih dana dobili poruku od CARNetove Abuse službe kako imate otvoren servis "portmapper", koji je predstavlja sigurnosni rizik, evo načina kako taj problem minimizirati, odnosno u potpunosti ga riješiti. Poruka koju smo dobili glasi otprilike ovako:

```
Postovani,

prilog sadrzi podatke o racunalima s aktivnim i javno dostupnim
Portmapper servisom.  Iako samo racunalo nije ranjivo pokrenuti
servis potencijalno moze biti iskoristen u DrDoS "amplification"
napadima. Dodatno moze biti iskoristen za pribavljanje velike
kolicine informacija o ciljanom uredjaju ako je dostupan program
"mountd".

Provjera dostupnosti portmapper servisa:

    rpcinfo -T udp -p [IP]

Provjera dostupnosti programa mountd:

    showmount -e [IP]
```

U prilogu maila se nalazi datoteka s opisom o kojem se računalu ili uređaju radi. Čemu ovaj servis uopće služi i trebamo li ga danas? Portmapper je servis za podršku RPC-u (Remote Procedure Call). Možemo ga promatrati i kao svojevrsni DNS server. Kada neka aplikacija želi uslugu nekog RPC servisa na vašem poslužitelja, pita rpcbind (fiksni port 111) na kojem portu i kojim protokolom (TCP, UDP) se može pristupiti usluzi. Rpcbind zna na kojem se portu servis nalazi, jer se prilikom starta sam proces registrirao u rpcbindu. Klijent se spaja na dojavljeni port i protokol i počinje s radom.

Od servisa koji koriste RPC najčešće će to biti NFS (Network File System, vidjeti https://en.wikipedia.org/wiki/Network_File_System), stariji Sunov protokol za montiranje udaljenih datotečnih sustava koji se i danas koristi. Cijela stvar zapravo nije previše komplicirana, pogledajte dijagram:




NFS je u CARNetovoj mreži pretpostavljamo i jedini servis koji bi eventualno mogao koristiti rpcbind, odnosno portmapper. Podsjetimo, nekada se servis nalazio u paketu "portmap", a od prije nekoliko godina dolazi u paketu "rpcbind" (koji donosi i virtualni paket portmap).

Ukoliko ste na svom poslužitelju izvršili naredbu "rpcinfo", mogli ste dobiti otprilike ovakav ispis:

```
# rpcinfo -p
   program vers proto   port  service
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  49211  status
    100024    1   tcp  57869  status
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100227    2   tcp   2049
    100227    3   tcp   2049
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100227    2   udp   2049
    100227    3   udp   2049
    100021    1   udp  34430  nlockmgr
    100021    3   udp  34430  nlockmgr
    100021    4   udp  34430  nlockmgr
```

```
    100021    1   tcp  48901  nlockmgr
    100021    3   tcp  48901  nlockmgr
    100021    4   tcp  48901  nlockmgr
    100005    1   udp  58467  mountd
    100005    1   tcp  55730  mountd
    100005    2   udp  33968  mountd
    100005    2   tcp  43627  mountd
    100005    3   udp  57306  mountd
    100005    3   tcp  44915  mountd
```

Na ovom poslužitelju se vrti servis portmapper/rpcbind, a također su eksportirani neki direktoriji, kojima mogu pristupiti neki udaljeni klijenti. To možemo provjeriti s naredbom "showmount":

```
# showmount -e
Export list for server:
/home/nfs
IP1,IP2,IP3
```

Eksportirani direktorij je /home/nfs, a poslužitelji kojima je dopušteno montirati te direktorije se nalaze na adresama IP1, IP2 i IP3.

Ukoliko imate eksportirane direktorije, vjerojatno koristite NFS i ne možete samo tako ugasiti rpcbind. Ovo govorimo u slučaju da ste tek naslijedili poslužitelj i još nije jasno što sve vrtite na njemu, a da nema potrebe za time.

Ukoliko ste sigurni da ne koristite NFS, onda nema potrebe ni za rpcbindom, pa ga možete obrisati:

```
# apt-get purge rpcbind
The following packages will be REMOVED:
rpcbind*
Do you want to continue [Y/n]? y
(Reading database ... 56206 files and directories currently installed.)
Removing rpcbind...
[ ok ] Stopping rpcbind daemon....
Purging configuration files for rpcbind ...
#
```

Ukoliko APT pita za nfs-* pakete, možete i njih obrisati. Ovime je vaš problem s nepotrebnim servisom i mailovima od Abuse službe riješen. No, što ako ne smijete obrisati rpcbind ili NFS?

Srećom, rpcbind podržava standardni tcp_wrappers, pa možemo zadati pristupnu listu, koji hostovi smiju pristupiti servisu, odnosno spriječiti da cijeli svijet vidi vaš portmapper. Ovo isto možete napraviti i pomoći iptablesa, ako vam je tako lakše.

Sve što trebate napraviti je upisati sljedeće u /etc/hosts.deny:

```
rpcbind: ALL EXCEPT IP IP1 IP2 IP3
```

IP je adresa vašeg poslužitelja, dok su ostalo adrese udaljenih klijenata. Da bi se promjene uvažile, najjednostavnije je restartati tcp_wrapper servis. Napomena: ova access lista označava koji se klijenti mogu spajati na servis rpcbind, a sam NFS ima svoju listu. Nemojte zaboraviti da rpcbind koristi i interface "lo", odnosno 127.0.0.1, ali on nije dostupan s Interneta i nije "opasan".

Sve što je ostalo je provjeriti situaciju sa poslužitelja kojima je dopušteno spajanje, te sa poslužitelja kojima to nije dopušteno. Ispis naredbe rpcinfo bi trebao biti ovakav na poslužiteljima kojima nije dopušteno spajanja (ili se servis ne vrti uopće):

```
# rpcinfo -T udp -p 161.53.X.Y
rpcinfo: can't contact portmapper: RPC: Remote system error - Connection refused
```

Jedna zanimljivost: rpcinfo opcija "-T", kojom definiramo "transport" (UDP ili TCP) se prijavljuje kao greška na poslužiteljima na kojima se ne vrti rpcbind. Isto je ako naredbu rpcinfo pokrenete, a niste root korisnik:

```
# rpcinfo -T -p 161.53.X.Y
rpcinfo: invalid option -- 'T'
```

Isto tako, taj "-T" iz maila Abuse službe se ne pojavljuje u manualu (man rpcinfo), iako smo opis pronašli online:

```
"Specify the transport on which the service is required. If this option is
not specified, rpcinfo uses the transport specified in the NETPATH
environment variable, or if that is unset or NULL, the transport in the
netconfig database is used. This is a generic option, and can be used in
conjunction with other options."
```

No, nije još kraj, na poslužiteljima na kojima opcija -T radi čini se da njena primjena uopće nema efekta (uvijek se ispišu i tcp i udp načini transporta). Pomalo čudno, ali eto, da vas ne iznenadi zašto opcija -T ne radi - jednostavno je izostavite.

čet, 2016-08-18 04:04 - Zdravko Rašić**Vijesti:** Linux [1]
**Kuharice:** Linux [2]
**Kategorije:** Servisi [3]
**Vote:** 5

Vaša ocjena: Nema Average: 5 (3 votes)

**Source URL:** https://sysportal.carnet.hr/node/1671

**Links**
[1] https://sysportal.carnet.hr/taxonomy/term/11
[2] https://sysportal.carnet.hr/taxonomy/term/17
[3] https://sysportal.carnet.hr/taxonomy/term/28