

Napredno korištenje operacijskog sustava Linux

3. Mrežni protokoli

Petar Šegina

Nositelj: doc.dr.sc. Stjepan Groš

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

26.03.2018

Sadržaj

- 1 Osnovni protokoli mrežne komunikacije - UDP i TCP
- 2 HTTP(S)
- 3 Upravljanje udaljenim računalom - SSH
- 4 Imenovanje računala - DNS
- 5 Upravljanje datotekama - SCP, FTP, FTPS, SFTP
- 6 Dinamično generirani sadržaj - (F)CGI
- 7 e-mail, kalendar i kontakti
- 8 Vrijeme - NTP
- 9 VPN

Mrežni protokoli

Open Systems Interconnection Reference Model

- Fizički sloj - Ethernet, USB, ISDN, 802.11, Bluetooth
- Podatkovni sloj - Ethernet, ARP, MAC, CSMA/CA
- Mrežni sloj - ICMP, IPsec, IPv4, IPv6, AppleTalk
- Transportni sloj - UDP, TCP
- Sjednički sloj - SOCKS, SAP, RTP
- Prezentacijski sloj - MIME
- Aplikacijski sloj - DNS, DHCP, FTP, HTTP, SMTP

Request For Comments

A Request for Comments (RFC), in the context of Internet governance, is a type of publication from the Internet Engineering Task Force (IETF) and the Internet Society (ISOC), the principal technical development and standards-setting bodies for the Internet. (...) RFCs have since become official documents of Internet specifications, communications protocols, procedures, and events.¹

¹https://en.wikipedia.org/wiki/Request_for_Comments

UDP i TCP

- Transportni protokoli izgrađeni nad IP - Internet Protocol
- Nisu jedini - SCTP, RDP, ...²
- User Datagram Protocol
 - RFC 768 - <https://tools.ietf.org/html/rfc768>
 - Jednostavan mehanizam slanja poruka među računalima
- Transmission Control Protocol
 - RFC 793 - <https://tools.ietf.org/html/rfc793>
 - Pouzdan, uređen, otporan na greške

²https://en.wikipedia.org/wiki/Category:Transport_layer_protocols

Poslužitelj i klijent

- netcat
 - (...) *a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol.*³
 - Poslužitelj
 - `nc -l {-u|--udp|-t|--tcp} -p 9998`
 - Klijent
 - `nc {-u|--udp|-t|--tcp} localhost 9998`
- telnet⁴
 - teletype network
 - RFC 15 - <https://tools.ietf.org/html/rfc15>
 - Klijent se može iskoristiti i kao TCP klijent
 - `telnet localhost 9998`

³man netcat

⁴<https://en.wikipedia.org/wiki/Telnet>

TLS - Transport Layer Security

- Protokoli koje smo naveli su jednostavni - i javno čitljivi
- Komunikaciju možemo zaštititi tako da prije pisanja i čitanja podatke kriptiramo
 - Sloj *omotač* oko prijenosnih protokola
- https://en.wikipedia.org/wiki/Transport_Layer_Security
- TLS v1.2 - RFC 5246 - <https://tools.ietf.org/html/rfc5246>

HTTP(S)

- Hyper Text Transport Protocol (Secure)
- TCP 80 i TCP 443
- RFC 2616 - <https://www.ietf.org/rfc/rfc2616.txt>
- Primjer ručnog slanja HTTP zahtjeva
 - `echo "GET / HTTP/1.0\n\n" | nc google.com 80`
 - Nakon nekoliko preusmjerenja dobivamo Google početnu stranicu
 - `echo "GET / HTTP/1.0\n\n" | nc google.com 443`
 - Ne dobivamo odgovor - Google očekuje zahtjev kriptiran TLS-om

Slanje TLS zahtjeva

- Ukoliko radimo ručno sa TCP, moramo sami odraditi i sav posao TLS-a
- openssl s_client - *SSL/TLS client program*⁵
 - `echo "GET / HTTP/1.0\n\n" | openssl s_client -ign_eof6
-connect google.com:443`

⁵man openssl s_client

⁶<https://stackoverflow.com/questions/19147280/how-do-you-pipe-echo-into-openssl>

curl i wget

- Za rad sa HTTP(S) poslužiteljima možemo koristiti i alate koji su izravno namijenjeni za to
- curl
 - *is a tool to transfer data from or to a server, using one of the supported protocols (DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMB, SMBS, SMTP, SMTPS, TELNET and TFTP)*⁷
- wget
 - *is a free utility for non-interactive download of files from the Web. It supports HTTP, HTTPS, and FTP protocols, as well as retrieval through HTTP proxies.*⁸
 - `wget -r --tries=10 http://fly.srk.fer.hr/ -o log`⁹

⁷man curl

⁸man wget

⁹man wget

Postavljanje vlastitog HTTP poslužitelja na internet

GitHub Student Pack

- <https://education.github.com/pack>
- Nudi mnogo korisnih alata za razvoj softvera
- Uključuje besplatnu .me domenu na Namecheapu
- Uključuje \$50 DigitalOcean kredita - dovoljno za 10 mjeseci jednostavnog poslužitelja
- Nije jedini izbor, ali je odličan za početi (jer je besplatan)



DigitalOcean

- <https://www.digitalocean.com/>
- Infrastructure-As-A-Service provider
- Kreiranje Virtual Private Servera unutar 60 sekundi na više lokacija na svijetu
- Naplaćivanje po satu¹⁰



¹⁰<https://www.digitalocean.com/pricing/>

Namecheap

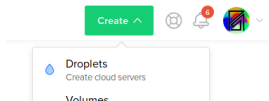
- <https://www.namecheap.com/>
- Popularan registar domena
- Omogućuje kupovinu i postavljanje mnogo različitih domena
- Nudi i besplatnu uslugu DNS posluživanja ¹¹



¹¹<https://www.namecheap.com/domains/freedns/>

Kreiranje virtualnog poslužitelja na DigitalOcean

- Kreirati *Droplet*



- Pričekati minutu

- *Droplet* je spreman za korištenje, a lozinka dolazi e-mailom

Hi, Petar Šegina

[Resources](#) [Activity](#)

DROPLETS (1)

  debian-s-1vcpu-1gb-fra1...	159.65.123.54	...
---	---------------	-----

Upravljanje udaljenim računalom - SSH

- Secure Shell protocol
- TCP 22
- RFC 4253 - <https://tools.ietf.org/html/rfc4253>

```
➔ ~ ssh root@159.65.123.54
root@159.65.123.54's password:
You are required to change your password immediately (root enforced)
Linux debian-s-lvcpu-lgb-fra1-01 4.9.0-6-amd64 #1 SMP Debian 4.9.82-1+deb9u3 (20
18-03-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Mar 23 14:49:04 2018 from 141.136.226.217
Changing password for root.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
root@debian-s-lvcpu-lgb-fra1-01:~#
```

SSH - dodatne funkcionalnosti

- `~/.ssh_config`¹²
- Autorizacija ključem
 - Autorizacija samo lozinkom nije sigurna
 - Može se u potpunosti onemogućiti kako bi se smanjila količina bruteforce pokušaja
 - <https://www.digitalocean.com/community/tutorials/how-to-use-ssh-keys-with-digitalocean-droplets>
 - Poslužitelju se nude svi lokalni ključevi
 - Problem za privatnost lokalnog stroja
 - Dobra ideja namjestiti `ssh_config` tako da poslužiteljima nudi lokalni ključ samo ako je tako deklarirano
- Port forwarding - <https://blog.trackets.com/2014/05/17/ssh-tunnel-local-and-remote-port-forwarding-explained-with-html>

¹²`man ssh_config`

SSH - izvršavanje skripti

- SSH možemo iskoristiti i kako bi izvršili skripte na udaljenom poslužitelju

```
ssh root@159.65.123.54 << HERE
    hostname;
    date;
HERE
```

SSH - poslužitelj

- Na poslužitelj se možemo spojiti putem SSH jer se na njemu izvršava SSH poslužitelj
- Primjerice, sshd - OpenSSH SSH daemon¹³

¹³man sshd

Poslužitelj nginx

- *a free, open-source, high-performance HTTP server and reverse proxy*¹⁴
- Jednostavan za uporabu i veoma brz
- `apt update && apt install nginx`
- nginx sada poslužuje HTML stranu sa `/usr/share/nginx/html/index.html`

¹⁴<https://www.nginx.com/resources/wiki/>

Let's Encrypt

- Naša strana je dostupna na internetu, ali nije zaštićena
- Da bi komunikacija s klijentima bila sigurna, potrebno ju je zaštititi TLS-om
- Potrebno je dobiti certifikat od nekog *Certificate Authorityja* kojem preglednici vjeruju
- Najjednostavnije (i besplatno) rješenje - Let's Encrypt¹⁵
 - Jednostavan za postaviti uz nginx¹⁶

¹⁵<https://letsencrypt.org/>

¹⁶<https://www.digitalocean.com/community/tutorials/how-to-secure-nginx-with-let-s-encrypt-on-ubuntu-16-04>

Imamo svoj kutak interneta!

(Ali nitko neće pamtititi našu IP adresu)

Imenovanje računala - DNS

- Domain Name System
- UDP 53
- RFC 1035 - <https://www.ietf.org/rfc/rfc1035.txt>
- Pohranjuje podatke o domeni
 - Koja je adresa poslužitelja za domenu? (A i AAAA)
 - Koji je mail poslužitelj za ovu domenu? (MX)
 - Pokazuje li ova domena na neku drugu? (CNAME)
 - Proizvoljan tekst vezan uz ovu domenu? (TXT)
 - i drugi¹⁷

¹⁷https://en.wikipedia.org/wiki/List_of_DNS_record_types

DNS upiti - alat dig

- *Domain Information Grouper*¹⁸
- *DNS lookup utility*¹⁹
- `dig @8.8.8.8 +noall +answer ANY fer.hr`
`fer.hr. 3422 IN A 161.53.72.119`
`fer.hr. 3422 IN SOA labs5.fer.hr. postmaster.labs5.fer.hr. 2018031301`
`fer.hr. 422 IN MX 1 fer-hr.mail.protection.outlook.com.`
`fer.hr. 3422 IN TXT "tWfeXfT/8d0+7Lpa5REWh3pASQErEh8gLqYU4hQ6u4VdJTY7t`
`fer.hr. 3422 IN NS labs5.fer.hr.`
`fer.hr. 3422 IN TXT "MS=34689B116A78E433D9BB3A222006AFE3F0010A5B"`
`fer.hr. 3422 IN NS sysdns.carnet.hr.`
- DiG HOWTO - <https://www.madboa.com/geek/dig/>

¹⁸<https://ns1.com/articles/decoding-dig-output>

¹⁹`man dig`

Može li i jednostavnije?

- */etc/hosts*
 - Jednostavno mapiranje IP adrese na hostname²⁰
 - Zgodan način za blokiranje određenih poslužitelja

²⁰man hosts

Kako postaviti svoju domenu?

Namecheap - postavljanje DNS upisa

SUPPORT ▾ psegina ▾  £0.00 ▾ 



Domains ▾ Hosting ▾ Apps ▾ Security ▾ Account ▾ 

 Dashboard

 Expiring /
Expired


 Domain List

 Product List

 Apps

 Profile

Domains → Details

 psegina.com

 Domain

 Products

 Sharing & Transfer

 Advanced DNS

HOST RECORDS

?

 Actions ▾

 Filters ▾

Search



<input type="checkbox"/> Type	Host	Value	TTL	
<input type="checkbox"/> A Record	@	37.187.121.25	Automatic	

Upravljanje datotekama - SCP, FTP, FTPS, SFTP

- Preko SSH možemo direktno uređivati datoteke na poslužitelju
 - No to nije praktično
- Za jednostavnije upravljanje datotekama na poslužitelju možemo koristiti neki od specijaliziranih protokola
 - SCP
 - *secure copy (remote file copy program)*²¹
 - Dolazi sa SSH - RFC 4251 - <https://tools.ietf.org/html/rfc4251>
 - Način korištenja sličan cp
 - `scp lokalna_datoteka.bin user@host:/usr/share/nginx/html/`
 - FTP(S)
 - RFC 959 - <https://tools.ietf.org/html/rfc959.html>
 - Potrebno podesiti FTP daemon na poslužitelju
 - Primjerice - `vsftpd`²²²³

²¹ `man scp`

²² <https://security.appspot.com/vsftpd.html>

²³ <https://www.digitalocean.com/community/tutorials/how-to-set-up-vsftpd-for-a-user-s-directory-on-ubuntu-16-04>

Upravljanje datotekama - SCP, FTP, FTPS, SFTP

- Za jednostavnije upravljanje datotekama na poslužitelju možemo koristiti neki od specijaliziranih protokola
 - SFTP
 - *SSH File Transfer Protocol*²⁴
 - Proširenje protokola SSH
 - Za razliku od SCP nudi i druge operacije nad datotečnim sustavom osim kopiranja

²⁴https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol

Dinamično generirani sadržaj - (F)CGI

- Možemo posluživati statičke datoteke, no kako posluživati dinamičan sadržaj?
- Common Gateway Interface
 - RFC 3875 - <https://tools.ietf.org/html/rfc3875>
 - Ne moramo svaki puta nanovo implementirati zaduženja HTTP poslužitelja
 - HTTP poslužitelj primi zahtjev
 - Pokrene naš program i na njegov standardni ulaz i okolinu pošalje primljene podatke
 - Ono što program ispiše na svoj standardni izlaz pošalje klijentu
 - Nedostatak - za svaki zahtjev stvara se novi proces
 - Proširenje - Fast CGI²⁵
- <https://www.howtoforge.com/serving-cgi-scripts-with-nginx-on-debian-squeeze-ubuntu-104-p3>

²⁵<http://www.mit.edu/~yandros/doc/specs/fcgi-spec.html>

e-mail, kalendar i kontakti

- e-mail

- Slanje - *Simple Mail Transfer Protocol*²⁶
- Pristup sandučiću - *Internet Message Access Protocol*²⁷ i *Post Office Protocol*²⁸
- Protokoli ne koriste TLS *po defaultu* - varijante SMTPS, IMAPS, POP3S, StartTLS²⁹

²⁶<https://tools.ietf.org/html/rfc5321>

²⁷<https://tools.ietf.org/html/rfc1730>

²⁸<https://tools.ietf.org/html/rfc1081>

²⁹https://en.wikipedia.org/wiki/Opportunistic_TLS

e-mail, kalendar i kontakti

- WebDAV

- *Web Distributed Authoring and Versioning*³⁰
- RFC 4918 - <https://tools.ietf.org/html/rfc4918>
- Proširenje HTTP-a koje omogućuje upravljanje dokumentima na poslužitelju
- CardDAV
 - *vCard Extensions to WebDAV*³¹
 - RFC 6352 - <https://tools.ietf.org/html/rfc6352>
- CalDAV
 - *Calendaring Extensions to WebDAV*³²
 - RFC 4791 - <https://tools.ietf.org/html/rfc4791>

³⁰<https://en.wikipedia.org/wiki/WebDAV>

³¹<https://en.wikipedia.org/wiki/CardDAV>

³²<https://en.wikipedia.org/wiki/CalDAV>

Vrijeme - NTP

- Svako računalo ima svoj sat
- Satove među računalima potrebno je sinhronizirati
- *Network Time Protocol*³³
 - RFC 958 - <https://tools.ietf.org/html/rfc958>
- Sinkronizacija pomoću lokalnih servisa
 - ntpd³⁴
 - systemd-timesyncd³⁵
- Važno je imati ispravno podešeno vrijeme, u suprotnom neke usluge mogu prestati ispravno raditi
 - TLS
 - DNS
 - e-mail

³³https://en.wikipedia.org/wiki/Network_Time_Protocol

³⁴<https://en.wikipedia.org/wiki/Ntpd>

³⁵<https://wiki.archlinux.org/index.php/systemd-timesyncd>

VPN

- *Virtual Private Network*
- Omogućava da se ponašamo kao da smo dio neke druge privatne mreže
- Možemo pristupati resursima samo unutar mreže
- Možemo pristupati vanjskim resursima šaljući zahtjeve iz te mreže
- Podiže razinu sigurnosti i privatnosti mrežnog pristupa
- OpenVPN - <https://openvpn.net/>
- <https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-16-04>

Kamo dalje?

- Na FER-u
 - Komunikacijske mreže³⁶
 - Mrežno programiranje³⁷
 - Raspodijeljeni sustavi³⁸
 - Osnove izrade PHP aplikacija³⁹
 - NKOSL - o mrežama i uslugama pričat ćemo još
- Beej's Guide to Network Programming⁴⁰
- Uz znanje dobiveno danas, pokušajte sami postaviti svoju web stranicu
 - Shameless plug - <https://pseгина.com>
 - Obavezno nam pošaljite link na nkosl@kset.org

³⁶<https://www.fer.unizg.hr/predmet/kommre>

³⁷<https://www.fer.unizg.hr/predmet/mrepro>

³⁸<https://www.fer.unizg.hr/predmet/rassus>

³⁹<https://www.fer.unizg.hr/predmet/oipa>

⁴⁰<https://beej.us/guide/bgnet/>

Literatura

https://en.wikipedia.org/wiki/Request_for_Comments
[https://en.wikipedia.org/wiki/Category:
Transport_layer_protocols](https://en.wikipedia.org/wiki/Category:Transport_layer_protocols)
<https://tools.ietf.org/html/rfc768>
<https://tools.ietf.org/html/rfc793>
<https://en.wikipedia.org/wiki/Telnet>
<https://tools.ietf.org/html/rfc15>
https://en.wikipedia.org/wiki/Transport_Layer_Security
<https://tools.ietf.org/html/rfc5246>
<https://www.ietf.org/rfc/rfc2616.txt>
[https://stackoverflow.com/questions/19147280/
how-do-you-pipe-echo-into-openssl](https://stackoverflow.com/questions/19147280/how-do-you-pipe-echo-into-openssl)

Literatura

<https://education.github.com/pack>
<https://www.digitalocean.com/>
<https://www.digitalocean.com/pricing/>
<https://www.namecheap.com/>
<https://www.namecheap.com/domains/freedns/>
<https://tools.ietf.org/html/rfc4253>
[https://www.digitalocean.com/community/tutorials/
how-to-use-ssh-keys-with-digitalocean-droplets](https://www.digitalocean.com/community/tutorials/how-to-use-ssh-keys-with-digitalocean-droplets)
[https://blog.tracks.com/2014/05/17/
ssh-tunnel-local-and-remote-port-forwarding-explained-with-ex
html](https://blog.tracks.com/2014/05/17/ssh-tunnel-local-and-remote-port-forwarding-explained-with-examples/)
<https://www.nginx.com/resources/wiki/>
<https://letsencrypt.org/>

Literatura

<https://www.digitalocean.com/community/tutorials/how-to-secure-nginx-with-let-s-encrypt-on-ubuntu-16-04>
<https://www.ietf.org/rfc/rfc1035.txt>
https://en.wikipedia.org/wiki/List_of_DNS_record_types
<https://ns1.com/articles/decoding-dig-output>
<https://www.madboa.com/geek/dig/>
<https://tools.ietf.org/html/rfc4251>
<https://tools.ietf.org/html/rfc959.html>
<https://www.digitalocean.com/community/tutorials/how-to-set-up-vsftpd-for-a-user-s-directory-on-ubuntu-16-04>
https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol
<https://tools.ietf.org/html/rfc3875>

Literatura

<http://www.mit.edu/~yandros/doc/specs/fcgi-spec.html>
<https://www.howtoforge.com/serving-cgi-scripts-with-nginx-on-debian-squeeze-ubuntu-11.04-p3>
<https://tools.ietf.org/html/rfc5321>
<https://tools.ietf.org/html/rfc1081>
https://en.wikipedia.org/wiki/Opportunistic_TLS
<https://tools.ietf.org/html/rfc4918>
<https://en.wikipedia.org/wiki/CardDAV>
<https://tools.ietf.org/html/rfc6352>
<https://en.wikipedia.org/wiki/CalDAV>
<https://tools.ietf.org/html/rfc4791>

Literatura

https://en.wikipedia.org/wiki/Network_Time_Protocol
<https://tools.ietf.org/html/rfc958>
<https://en.wikipedia.org/wiki/Ntpd>
<https://wiki.archlinux.org/index.php/systemd-timesyncd>
<https://openvpn.net/>
<https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-16-04>
<https://beej.us/guide/bgnet/>