

## ● Sadržaj

- Napomena
- Relativna sigurnost u BSD-u i GNU/Linux-u
  - Šifre moraju biti veoma jake
  - Ključevi moraju biti jedinstveni
  - Nigde ne ostavljajte svoje lične podatke, jer Internet sve pamti
  - Kako paketi putuju po Internet mreži
  - Društvene mreže
  - Bruce Schneier
  - Replay attacks
  - Virusa ima i za BSD i GNU/Linux
  - Zlonamerne skripte
    - Neželjeni procesi
    - Fork bomb
    - Kako da namestite limite
  - Ako neko ima fizički pristup Vašem kompjuteru
  - Šta se dešava ako hackeru ukradete kompjuter
    - Prey
  - FreeBSD Kernel i GNU/Linux Kernel nisu uvek sigurni
  - Sistem uvek treba da bude aktuelan
  - Zaštitite prepisku svake vrste preko Interneta
  - Postavite zaštitni zid
- Zaštita od nepoželjnih logovanja, to jest napada na Vaš sistem
  - TCP-Wrappers
  - Tcpcrypt
  - Kako zaštititi DNS
    - OpenDNSSEC
    - Unbound
    - P2P DNS
  - Dodatni programi za sprečavanje nepoželjnih logovanja
    - Deny Hosts
    - psad
    - Fail2ban
    - PortSentry
    - SSHGuard
- Zaštitni zid, Firewall
  - Zaštitni zid, Firewall za BSD
    - PF, The OpenBSD Packet Filter
    - IPFW, The IPFIREWALL
    - IPF, IP Filter
  - Zaštitni zid, Firewall za GNU/Linux
    - Iptables / Netfilter

- [GUI za Firewall](#)
    - [FW Builder](#)
    - [Qtfw](#)
  - [Koja aplikacija koji Port normalno koristi](#)
  - [Kako da neki Port propustite](#)
  - [Neki Port niste otvorili, ali ih neki Program otvara](#)
  - [Precizno podešavanje zaštitnog zida preko GUI-a nije moguće](#)
  - [Kako da pravite Iptables pravila](#)
  - [Sa zaštitnim zidom sve zabraniti](#)
  - [Ne isključivati zbog jednostavnosti ili lakoće zaštitni zid od Router-a](#)
  - [Većinom su napadi upereni na na Port 22 TCP a to je SSH](#)
  - [Za ovo sve ne postoje GUI već se mora raditi u konzoli](#)
  - [Firewall skripta /etc/rc.firewall](#)
  - [Da bi to mogli koristiti GeolP za Firewall i kontrolu](#)
- 
- [Kontrola](#)
    - [Posetite obavezno ove i ostale stranice koje pišu o sigurnosti](#)
    - [Ne koristite za pretraživanje Interneta Google](#)
    - [Redovno pregledajte sistemske log fajle](#)
    - [Koji programi postoje za kontrolu](#)
      - [Kako se koriste ovi programi](#)
        - [Portovi](#)
        - [Konekcije](#)
        - [Hosts](#)
        - [MAC adrese](#)
      - [Obavezno obnavljajte sistem](#)
- 
- [Kontrola u X-u](#)
    - [Conky](#)
    - [GKrellM](#)
    - [System Monitor](#)
    - [QtSystemInfo](#)
    - [KSysguard](#)
    - [Nagios](#)
- 
- [SSH protokol](#)
    - [OpenSSH](#)
    - [Dodatni programi za SSH protokol](#)
      - [Keychain](#)
      - [Autossh](#)
      - [ScanSSH](#)
      - [SecPanel](#)
      - [Putty](#)
      - [rssh](#)
      - [scponly](#)
    - [Ključevi za OpenSSH](#)
      - [Više ključeva za različite mreže](#)

- [Prenošenje SSH ključeva](#)
  - [SSH-installkeys](#)
  - [Podprogram od OpenSSH-a](#)
  - [Manuelan način prenošenja SSH ključeva](#)
- [Primer podešavanja za OpenSSH](#)
  - [Fajla ~/.ssh/config](#)
  - [Fajla ~/.ssh/authorized\\_keys](#)
- [SSH Tunnel](#)
- [Upotreba OpenSSH-a](#)
  - [Obaveštenja prilikom SSH logovanja na Vaš kompjuter](#)
  - [Logovanje preko SSH-a](#)
  - [Potrebno je da ograničite korišćenje root naloga za OpenSSH](#)
- [FUSE, Filesystem in Userspace](#)
  - [SSHFS, SSH Filesystem](#)
  - [SMBNetFS](#)
  - [SMB for Fuse](#)
- [Šifrovanje i upotreba GNU Privacy Guard-a, zamena za PGP](#)
  - [Kratka istorija GnuPG](#)
  - [Programi za GnuPG](#)
    - [GnuPG The GNU Privacy Guard](#)
      - [GPGTools](#)
      - [Pinentry](#)
      - [GUI za GnuPG](#)
        - [GPA, GNU Privacy Assistant](#)
        - [Seahorse](#)
        - [GnuPG-Interface](#)
        - [Kpgp](#)
        - [gpg-ringmgr](#)
        - [GnuPG Shell](#)
      - [GnuPG za Windows](#)
        - [GnuPG for Windows](#)
        - [WinPT](#)
        - [GPGol, GNU Privacy Guard Microsoft Outlook](#)
        - [GPGee, GNU Privacy Guard Explorer Extension](#)
        - [Prevođenje sa MinGW](#)
      - [Uputstva kako koristiti GnuPG za BSD, GNU/Linux i Windows](#)
      - [Ključevi za GnuPG](#)
        - [Pravljenje ključeva za GnuPG preko konzole](#)
        - [Pravljenje ključeva za GnuPG preko GUI-a](#)
        - [Razmena GnuPG ključeva](#)
        - [Davanje javnih ključeva na Server](#)
        - [Dodavanje identiteta u GnuPG ključ](#)
        - [Brisanje GnuPG ključeva](#)
      - [Razne ostale komande sa rad sa GnuPG-om](#)
      - [Da bi GnuPG-Agent radio u konzoli i u X-u](#)

- [Kako zaštiti Instant Messaging i Internet Live Conferencing](#)
  - [Koju zaštitu za Instant Messaging koristiti](#)
    - [OTR \(Off-the-Record Messaging\)](#)
    - [End to End message Encryption](#)
  - [Koju zaštitu za Internet Live Conferencing koristiti](#)
    - [FiSH](#)
      - [FiSH upotreba](#)
      - [MIRACL](#)
    - [Mircryption](#)
- [Zaštitite Vaše šifre](#)
  - [KeePassX](#)
  - [YAPET, Yet Another Password Encryption Tool](#)
  - [Gringotts](#)
  - [wmpasman](#)
  - [Password Safe](#)
    - [Java PasswordSafe](#)
    - [cliPSafe](#)
    - [Gorilla](#)
- [Zaštita od virusa](#)
  - [ClamAV](#)
    - [ClamTk](#)
    - [ClamAV Unofficial Signatures Updater](#)
    - [ClamFS](#)
    - [clamd-stream-client](#)
  - [AMaViS, A Mail Virus Scanner](#)
    - [amavisd-new](#)
    - [amavisd-milter](#)
    - [amavis-logwatch](#)
    - [amavis-stats](#)
  - [F-PROT](#)
  - [Penguin Pills](#)
  - [Dazuko](#)
- [Kriptovanje fajli](#)
  - [Kriptovanje fajli sa GnuPG](#)
  - [bcrypt](#)
  - [Možete kriptovati istovremeno sa GnuPG i bcrypt](#)
  - [bdes](#)
  - [ccrypt](#)
  - [Elettra](#)
- [Cryptographic hash function](#)
  - [md5](#)
  - [md5sum](#)

- [md5deep](#)
- [Isomd5sum](#)
- [Steganografija](#)
  - [Steghide](#)
- [SSH, Kernel, Iptables, patch-o-matic](#)
  - [Iptables se mora obnoviti pre bilo kakvog patch-ovanja](#)
  - [Kernel patch-ovanje](#)
  - [Iptables patch-ovanje](#)
- [NFS protokol, Network File System](#)
  - [NFS za BSD](#)
  - [NFS za Debian GNU/Linux](#)
  - [NFS za Gentoo](#)
  - [Primer za NFS klijenta](#)
  - [Primer za NFS Server](#)
  - [Sigurnost za NFS](#)
  - [Ako imate probleme sa NFS-om](#)
- [Upotreba Rsync-a](#)
  - [Možete koristiti root nalog za OpenSSH samo za restriktivni Rsync](#)
  - [Grsync](#)
  - [rdiff-backup](#)
  - [Lsyncd](#)
- [NAS, Network-Attached Storage](#)
  - [FreeNAS](#)
  - [OpenMediaVault](#)
- [SSL protokol](#)
  - [OpenSSL](#)
  - [NSS, Network Security Services](#)
  - [Common CA Certificates](#)
  - [create-cert](#)
  - [TinyCA](#)
  - [Ručno podešavanje OpenSSL-a](#)
- [FTP protokol, File Transfer Protokol](#)
  - [vsftpd, Very Secure FTP Deamon](#)
    - [Podešavanja za vsftpd, Very Secure FTP Deamon](#)
  - [LFTP](#)
  - [gFTP](#)
  - [KFTPgrabber](#)
  - [FileZilla](#)

- [Layer 5](#)
- [Radius protokol, Remote Authentication Dial In User Service](#)
- [VPN protokol, Virtual Private Network](#)
  - [OpenVPN](#)
- [Povezivanje pomoću tunela](#)
  - [HTTP tunnel](#)
  - [Stunnel](#)
  - [Proxytunnel](#)
  - [VTtun, Virtual Tunnel](#)
  - [Zebedee](#)
  - [Dnsmasq](#)
  - [IMSpecator](#)
- [Povezivanje preko X protokola](#)
  - [Ako imate više kompjutera a jednu tastaturu i jednog miša](#)
  - [Preko SSH protokola na udaljeni X](#)
  - [VNC protokol, Virtual Network Computing](#)
    - [VNC alatke](#)
    - [Upotreba VNC-a](#)
  - [NX protokol](#)
  - [Linux Terminal Server Project](#)
  - [RDP protokol, Remote Desktop Protokol](#)
  - [GUI za razne protokole](#)
  - [Ostala rešenja za povezivanje preko X protokola](#)
- [Kontrolisanje tastature i miša](#)
  - [Xnee](#)
  - [PyKeylogger](#)
  - [logkeys](#)
  - [LKL](#)
- [Centralno održavanje više kompjutera](#)
  - [Webmin](#)
  - [ClusterSSH](#)
  - [PSSH, Parallel SSH Tools](#)
  - [Tentakel](#)
  - [shmux](#)
  - [Mussh](#)
  - [Pdsh, Parallel Distributed Shell](#)
  - [Polysh](#)
  - [KontrolPack](#)
  - [Unison](#)
  - [Duplicity](#)
  - [MCollective, Marionette Collective](#)
- [Samba protokol](#)

- [Samba](#)
- [SambaScanner](#)
- [PPTP Protokol, Microsoft Point-to-Point Tunneling Protocol](#)
- [Kombinovana rešenja za razne protokole](#)
- [Smartcard](#)

## **Napomena**

U [primerima](#) imate sve skripte i fajle ovde navedene, posebno one iz /home/bin su kompletno tu.

Za skoro sve ovde opisane programe stavio sam u [Fluxbox menu](#) kako se startaju, takođe u [primerima](#) imate i taj menu. Iz tog razloga nisam opisao ovde kako se koji program starta, mnogi imaju svoj specifičan način startanja.

Ako koristite drugo [grafičko okruženje](#) svejedno pogledajte taj menu, jer opisano je kako se startaju programi, pa možete to dodati u Vaš meni ili ih tako ručno startati.

## **Relativna sigurnost u BSD-u i GNU/Linux-u**

Da vidite šta ima za [BSD](#)

```
cd /usr/ports/security/ ; ls
```

Pogledajte [Zdravlje](#), dosta je slična problematika na svim poljima.

<http://www.elitesecurity.org/t339823-Relativna-sigurnost-Linux>

<http://www.conwex.info/draganp/>

<http://blog.b92.net/blog/10675/Dragan-Pleskonjic/>

<http://www.certicom.com/index.php/an-introduction-to-the-uses-of-ecc-based-certificates>

<http://privacyalternatives.wikispaces.com/>

**BSD i GNU/Linux jesu relativno sigurniji po default-u od [smopu!M-a](#),**

**ali ništa nije potpuno sigurno.**

**Ne treba se zanositi sa osećajem sigurnosti u BSD i GNU/Linux-u, a posebno ne u smopu!M-u. Stvarnost je drukčija.**

**Put da se od normalnog korisnika Interneta postane stakleni čovek je vrlo lako da se pređe. Mnogi ni ne vide da su dali sve o sebi na Internet. Da se pravi Vaš profil, da se zna sve o Vama, što Vi ni ne zнате da neko može znati.**

**Na internet, preko preglednika, email programa i za ostale normalne delatnosti, sme da ide samo normalni korisnik, za igre i eventualno emulatore korisnik za igre i emulatore, nikako administrator (root)!**

<http://packetstormsecurity.org/>

<https://www.securelist.com/en/>

Koliko zvanični izvori vole enkripciju

<http://publicintelligence.net/do-you-like-online-privacy-you-may-be-a-terrorist/>

Čak i filtrovani izvori daju dobre informacije, koje ne mogu da se sasvim sakriju od javnosti

[https://en.wikipedia.org/wiki/Secure\\_communication](https://en.wikipedia.org/wiki/Secure_communication)

[https://en.wikipedia.org/wiki/Deniable\\_encryption](https://en.wikipedia.org/wiki/Deniable_encryption)

## **Šifre moraju biti veoma jake**

**Svakom napadaču je najbitnije kad dobije pristup u sistem, da dobije root šifru.**

**A kad dobije šifru može svašta da radi, da instalije Rootkit-ove, promeni ELF fajle tako da prvo izvrše njihov kod pa tek onda kod od programa koji je inficiran.**

**Mogu menjati i logovanje, da izbrišu sve svoje tragove u**

**/var/log/messages i ostalim fajlama nećete naći ništa što je sumnjivo.**

**Može koristiti Vaš kompjuter za napada na druge kompjutere...**

**Zbog toga poželjna je jaka šifra za administratora i korisnike, ključeve za OpenSSH.**

**Mora biti od najmanje 15 znakova do koliko hoćete (predlog 20 do 30), što više to bolje, sa velikim, malim slovima, brojevima, znakovima interpunkcije, menjati je svaka 2 do 4 meseca.**

**Jednostavno a veoma lako je za zapamtiti neki Vama poznat izraz. Promenite samo mala slova ponegde u velika, poneki broj i znak interpunkcije. Naravno ovo**

**Iako može da bude veoma duga rečenica, ali koja se lako pamti. ☺**

**Možete koristiti neku samo Vama poznatu dugu rečenicu i da koristite samo iz nje početna ili zadnja slova reči i da kombinujete to sa velikim i malim slovima, brojevima, znakovima interpunkcije.**

**Ako je to više od 20 znakova onda budite sigurni da će neko veoma teško ili nikad neće moći da ih razbije i ne morate tako često to menjati, ali ne dajte to nikom na uvid.**

**Koristite za svaku Internet stranicu ili servis, drugo ime i šifru.**

<http://world.std.com/~reinhold/diceware.html>

**Šifre kako to gledaju napadači**

<http://www.bitflop.com/document/101>

**Ne koristite ni slučajno ovo ili nešto slično, gde Vam naizgled olakšava da nemate više šifri, ali zato ide u pravcu staklenog čoveka**

<http://openid.net/get-an-openid/>

**Kako da ispitate šifre**

[http://tools.question-defense.com/Cracking\\_Passwords\\_Guide.pdf](http://tools.question-defense.com/Cracking_Passwords_Guide.pdf)

**Pogledajte [kraj ovog Podsetnika](#), Zaštitite Vaše šifre, John the Ripper.**

<https://www.xkcd.com/936/>

<https://miloske85.wordpress.com/category/computer/>

Zato promenite odmah Vaše šifre

**su**

**passwd**

**passwd user**

**Ključevi moraju biti jedinstveni**

**Kompjuter mora biti zauzet dok pravite bilo koje ključeve. Onda će se Vaši ključevi i brzo napraviti.**

**Neka bude i 80% zauzet CPU, to je izvanredno za pravljenje ključeva.**

**Možete dati i ovu komandu, ona je posebno efikasna.**

**du -hs /**

**Mrdajte mišem, pišite nešto na tastaturi, u nekom tekstualnom dokumentu, prevodite neki program, bilo šta samo da je što više zauzet procesor.**

**Treba uvek da se nasumice (random) generiše ključ.  
Onda će biti jedinstven (unicus).**

**Istovremeno će brže da se generiše ključ.**

**Koristite to za svako pravljenje ključeva na primer za  
VPN, Pidgin, Gajim, GnuPG, OTR...**

**Nigde ne ostavljajte svoje lične podatke, jer Internet sve pamti!**

**A ako baš morate dobro pazite gde ste ostavili i radite samo preko https protokola.**

**Mada ni to nije sasvim sigurno.**

**Koristite gde god možete zaštitu da se sva Vaša komunikacija šifruje i da se ne može pročitati tako lako. Jer ko zna kojim sve putevima putuje neka Vaša poruka.**

**Koristite samo Free Software programe, koja imaju otvoren kod, koji niko ne može promeniti a da se ne primeti skoro istog trenutka.**

**Ako ste stvarno nešto zgrešili, onda teško da Vas neka zaštita može spasiti.**

Ako na više strana ostavite Vaše podatke napadač može napadač, koji hoće da Vam naudi, da napravi veoma lako Vaš profil.

Pazite ako koristite neku email listu, znajte da se to pamti na više mesta.

Ne stavljamte svoje slike i adrese na Internet. Pazite šta pišete na IRC-u i raznim Chat-ovima.

Koristite razne Nick-ove, šifre za svaku Internet stranu što posećujete, barem za grupu strana, mada je najbolje da se sve totalno razlikuje, da koristite svaki dan i uvek [sakrivanje IP adrese](#) na svim stranama.

Mora biti izuzetak od pravila kad dajete svima na znanje Vašu IP adresu.

To je veoma opasno mada komforno jer se onda povećava brzina Interneta, ali bitnija je sigurnost a ne brzina.

Informacije sa tih strana i rezultati od mašina za pretraživanje interneta mogu napraviti Vaš profil veoma detaljano i tačno se može odrediti gde i kako živite, koje su Vam naklonosti, sa kim živite, kako živite, koje su Vam naklonosti, koje životinje imate i još puno puno toga...

Naći se može samo oni podaci koje ste Vi na bilo koji način ostavili na internetu.

Internet saobraćaj se uvek na više mesta prisluškuje (vlade, manje ili više tajne službe, razne agencije, hackeri, crackeri, maštine za pretraživanje...) i skoro sve se pamti, obrađuju i prodaju se informacije zainteresovanim.

Neko će da kaže:

Što ja moram da se štitim, ja i onako ništa ne radim nezakonito, ima već koga će oni da kontrolišu i napadaju.

To je tako bespotrebno, bezvezno i teško, što ja moram paziti i instalirati neke preterane zaštite. Neće mene niko napadati jer ja ništa ne radim što ne bi trebalo.

**Na baš takve koji se ne brinu oko zaštite čekaju razne organizacije i Hackeri.**

**Nažalost ima puno ljudi koji ne shvataju koliko je važna sigurnost.**

<http://blog.b92.net/text/16866/Carobni-stapic/>

U [BSD](#) i [GNU/Linux](#)-u je bolja zaštita nego u [smopu!M](#)-u. Ali moguće je i u [smopu!M](#)-u se donekle zaštiti, mada dosta teže, jer sam sistem je loše napravljen.

Imate primere kako da koristite [Free Software](#) programe, na primer

Sa [GnuPG](#) ključevima [Claws Mail](#), [Gajim](#), [Psi](#), [Mcabber](#)...

[OTR](#) autentifikaciju mogu koristiti ovi programi [Pidgin](#), [Gajim](#), [Psi](#), [Kopete](#), [MCabber](#)

A preko i [Irssi-otr](#) i [Irssi](#), [XChat](#), [WeeChat](#), [BitlBee](#)

Koristite uvek sve šta možete, ali ne preterujte puno sa različitim vrstama zaštite za isti problem. Da ne bude kao da imate više AntiVirus-a koji se međusobno kolju a Virusi kolo vode, lep primer iz [smopu!M](#) sveta.

## Kako paketi putuju po Internet mreži

Malo šaljivo, ali nije daleko od istine

[http://www.youtube.com/results?search\\_query=How+Internet+Traffic+Works+\[Warriors+of+the+Net\]](http://www.youtube.com/results?search_query=How+Internet+Traffic+Works+[Warriors+of+the+Net])

## Društvene mreže

**Ne preporučujem da koristite Facebook, Google+, Twitter, Myspace, Paltalk, Dropbox, zatvorene protokole za IM niti bilo šta slično.**

**Naravno izbor je na Vama da li ćete koristiti društvene mreže ili nećete, to je Vaš lični izbor.**

**Takođe nije preporučljivo da koristite takozvane igre koje zamenjuju delimično realni život.**

**Mogu se i ovakve stranice donekle štititi sa HTTPS Everywhere, ShareMeNot i CookieCuler dodatkom za Mozilla preglednike.**

**Uvek pre nego što pritisnete dugme ili šta slično da se slažete sa pravilima, dobro pročitajte kompletna pravila date stranice ili ugovora, najbitnije je što je sitno napisano.**

Korisnici Facebooka zatiču na **Zidu** poruku koju je navodno ostavio neki od njihovih prijatelja; poruka obično sadrži hipervezu do neke Web lokacije ili video odlomka.

Radi se o tome da zlonamernici koriste lakovernost neopreznih korisnika Facebooka koji ne sumnjaju u takvu poruku, za razliku od poruke sa hiperezom koja im odnekuda stigne e-poštom.

Kada neoprezni korisnik Facebooka pritisne hiprevezu, ona ga vodi do lažne Web lokacije gde se od njega traži da ostavi poverljive lične podatke.

Mogu da se uključe sigurnosne opcije ali to ne pomaže mnogo.

Uvek onaj koji je napravio stranicu može da radi šta hoće sa njom, da prodaje Vaše podatke gde god i kome god hoće.

Često se jednostavno pritisne dugme **I like this**, iako se stvarno ne zna šta to znači i koje sve posledice može to da donese.

**Ima puno primera kako se društvene mreže mogu zloupotrebiti**

Ljudi koji imaju dosta psihološkog iskustva, mogu da naprave profil i da tačno obrade neku osobu. To isto rade i razne službe i firme, na primer [Echelon](#).

Jedan čovek Milan je imao problema da zadobije neku devojku preko Interneta. Nikako mu to nije uspevalo, ma šta da je radio. Požali se Mladenom koji se razume u psihologiju i kaže koji problem ima. Dao mu na uvid sve njene podatke koje je imao.

Mladen je koristio ime i prezime, datum rođenja, natalnu kartu (horoskop) i ostalo šta je bilo na Internetu o njoj.

Onda ona sa upotrebom tih podataka uzme Milana za prijatelja na Facebook-u.

Tada ode Mladen sa Milanovim nalogom na Facebook i napravi njen psihološki profil, šta voli, šta ne voli i tako dalje. Kasnije je Mladen samo rekao Milanu šta treba da uradi da bi je zadobio za sebe, to jest na šta ona pada. Onda je samo bilo pitanje dana da se to i desi.

Kako je privatnost na nivou i kako Facebook koristi Vaše kolačice

<http://www.index.hr/vijesti/clanak/nova-povreda-privatnosti-facebook-prati-vase-internetske-aktivnosti-i-nakon-sto-se-odlogirate/573747.aspx>

**Znajte da kriminalci plaćaju velike sume da zaznaju lične podatke, a posebno ako je u njima broj nekog konta.**

Na sličan način se odvijaju i hakerski napadi.

Hiperveze koje se u tom slučaju koriste obično vode do hakerskih Web lokacija, gde se korisniku nudi da preuzme neku datoteku iza koje se ustvari krije trojanac koji na napadnutom računaru instalira zlonamerni softver, što omogućava napadaču da ostvari potpunu kontrolu nad napadnutim računaram.

**Ima različitih alata na Internetu tražite na primer FacebookPWHack.exe...**

A često se Vaši podaci ne brišu iako izbrišete kontakt. Morate sami obrisati sve Vaše podatke, kao slike, poruke i šta god ste ikad uneli na [Društvene mreže](#).

Ove stranice Vas mogu samo informisati, to niko sem Vas ne može da uradi. Dobro prvo sve pročitajte na njima, pa tek onda krenite u brisanje podataka pa tek onda kad ništa više nemate od Vaših podataka brišite korisnički nalog.

<http://www.wikihow.com/Quit-Facebook>

<http://www.infinius.hr/blog/virtualno-samoubojstvo-obrisi-me-zauvijek/>

<http://gizmodo.com/5530178/top-ten-reasons-you-should-quit-facebook>

Možete koristiti ove stranice, ali bolje je da sami to pokušate uraditi pa tek ako to ne uspe onda probati da ih koristite

<http://suicidemachine.org/>

Ova stranica je nastala posle otkrića propusta u privatnosti Facebook-a

<http://www.quitfacebookday.com/>

## Bruce Schneier

Odlična stranica o sigurnosti

<http://www.schneier.com/>

Delovi su prevedeni je na više jezika

<http://www.schneier.com/bylanguage.html>

Možete se prijaviti na mesečnu Crypto-Gram listu.  
Preporučujem ako se zanimate za sigurnost.

<http://www.schneier.com/crypto-gram.html>

Bruce Schneier je napisao program Password Safe.

## Replay attacks

I pored zaštite uvek postoji mogućnost napada pri uspostavi veze od Replay attacks.

Prisluškivanje zaštićenog saobraćaja, najbolje u vreme kad je malo saobraćaja, analiza i nalaženje vitalnih podataka, na primer koji paketi predstavljaju prenos novca i tako dalje i usmereni napad posle.

Napadač ne mora da zna uopšte način zaštite, samo mora biti u mogućnosti da reprodukuje te pakete. Ko ne koristi zaštitu od ponovljenih napada biće zagušen sa tim paketima.

Known plaintext attacks, poznatih otvorenih napada

To znači moguće je izvesti MITM (Man in the middle) napade u skoro svako vreme i svuda.

Relativna sigurnost u BSD-u i GNU/Linux-u

Šifre moraju biti veoma jake

Ključevi moraju biti jedinstveni

Nigde ne ostavljajte svoje lične podatke, jer Internet sve pamti

[Društvene mreže](#)

[Bruce Schneier](#)

[Replay attacks](#)

[Virusa ima i za BSD i GNU/Linux](#)

[Zlonamerne bash skripte](#)

[Sistem uvek treba da bude aktuelan](#)

[Zaštitite prepisku svake vrste preko interneta](#)

[Postavite zaštitni zid](#)

[Na početak](#)

## **Virusa ima i za BSD i GNU/Linux**

**Nije samo smopu!M ugrožen, mada on jeste najviše napadan.**

Pogledajte [Zaštita od virusa.](#)

Pogledajte dobro ove stranice

<https://duckduckgo.com/> Virus+BSD

<https://duckduckgo.com/> Virus+Linux

<http://www.spamlaws.com/first-linux-virus.html>

[GNU/Linux Virus-i i Malware](#)

[https://en.wikipedia.org/wiki/Linux\\_malware](https://en.wikipedia.org/wiki/Linux_malware)

Heise online

<http://www.heise.de/newsticker/SCO-vs-Linux-Virus-auf-Zeitreise--/meldung/44182>

Upozorenje za [GNU/Linux](#) viruse

<http://www.urz.uni-heidelberg.de/security/system/linuxvirus.html>

Erkennung des Virus Linux/Rst-B

<http://www.pro-linux.de/berichte/linux-virus-rst-b.html>

Antivirus solutions for [GNU/Linux](#)...

<http://www.linux.com/articles/22899>

Takođe ima i Rootkit-ova, Trojanaca, Malware.

Linux Trojan gets closer look...

<http://www.vnunet.com/vnunet/news/2116024/linux-trojan-gets-closer-look>

[http://www.linuxzasve.com/clanak/sigurnosne\\_prijetnje\\_linux\\_pocetnicima/53](http://www.linuxzasve.com/clanak/sigurnosne_prijetnje_linux_pocetnicima/53)

<http://laptoplogic.com/resources/understanding-and-avoiding-malicious-code-attacks-in-linux>

[http://linuxreviews.org/gentoo/gentoo\\_trojan\\_howto/](http://linuxreviews.org/gentoo/gentoo_trojan_howto/)

## Zlonamerne skripte

**Ne preuzimajte nikakve skripte sa interneta a posebno ne sa IRC-a i uvek proverite šta one stvarno rade. Koje su komande unutra.**

**Nikada ne izvršavajte neproverene skripte kao [root](#).**

**Zlonamerni "takozvani Hakeri" ali ustvari "Crakeri" hoće sa ovakvim bash skriptama da Vam unište kompjuter.**

**Ovo briše /var /root /etc...**

```
cd / && eval `ls --color=never -1 / | grep "lost+found" | tr "Istound+" " m r * -`
```

ili

```
cd / && eval `ls --color=never -1 / | grep "lost+found" | tr "Istound+" " m r * -`
```

**Nemojte nikad da koristite komandu!**

```
rm -rf /
```

Ako koristite [tcsh](#) stavite da dobijete uvek pitanje da li da brišete u

/etc/csh.cshrc

```
# Ask for confirmation when 'rm *'  
set rmstar
```

## A ovde imate razne skripte koje uništavaju sistem

<http://www.junauza.com/2008/11/7-deadly-linux-commands.html>

## Neželjeni procesi

Da možete ubiti zombi procese koji se javljaju na neki način u Ubuntu-u i loguju, možete koristiti ovu skriptu

```
/home/bin/kill-zeitgeist
```

## Fork bomb

[https://secure.wikimedia.org/wikipedia/en/wiki/Fork\\_bomb](https://secure.wikimedia.org/wikipedia/en/wiki/Fork_bomb)

<http://www.cyberciti.biz/faq/understanding-bash-fork-bomb/>

<http://mywiki.wooleedge.org/BashFAQ/059>

Koči ceo sistem jer se stalno procesi umnožavaju

```
:() { :|:& };
```

```
:() { :|: & }::
```

Ili kao C++ program

```
#include <iostream>  
using namespace std;
```

```
int main()
{
    for (int i = 0; i<100000; i++)
    {
        for (int l = 0; l<10000000; l++)
        {
            cout << "BYE";
            system("du / &");
            system("soffice &");
            cout << 101010101011100101 + l + i / i + i / l + 1216515615156;
            cout << i + i * 545564 + 2512 - 2 + 1 * 1000 / 5;
        }
    }
    return 0;
}
```

```
#include <unistd.h>

int main()
{
    while(1)
        fork();
}
```

```
#include <iostream>
#include <unistd.h>
#include <cstdlib>

using namespace std;

int main ()
{
    for (int i = 0; i<250; i++)
    {
        cout << "Process: ";
        system("ps aux | grep stefan | wc -l");
        cout << endl;
        fork();
    }
    return 0;
}
```

```
void func() {func();} int main() {func(); return 0;}
```

## Kako da namestite limite

Pogledajte [Kako BSD i GNU/Linux koriste memoriju.](#)

Možete da sprečite [Fork bomb](#) kao i ostalo

<http://www.gentoo.org/doc/en/security/security-handbook.xml?part=1&chap=5>

<http://www.cyberciti.biz/tips/linux-limiting-user-process.html>

Morate znati koliko imate otvorenih procesa i otvorenih fajli ukupno

```
ps aux | wc -l
```

```
lsof | wc -l
```

Za [root](#)-a

```
ps aux | grep root | wc -l
```

```
lsof | grep root | wc -l
```

Za Vašeg [normalnog korisnika](#)

```
ps aux | grep normalni-korisnik | wc -l
```

```
lsof | grep normalni-korisnik | wc -l
```

To sve vidite sa skriptama

```
/home/bin/ps-
```

```
/home/bin/lsof-
```

Najbolje je da obe opcije koristite imali ili nemali PAM

Nikad se ne zna, ovo je osnovno za zaštitu

## Ako koristite PAM

Za [GNU/Linux](#)

Podesite konfiguraciju

<http://linux.die.net/man/5/limits.conf>

<http://ss64.com/bash/limits.conf.html>

/etc/security/limits.conf

## Ako ne koristite PAM

Kako da ograničite upotrebu resursa

Za [BSD](#)

/etc/login.conf

man login.conf

<http://www.freebsd.org/doc/handbook/users-limiting.html>

<http://freebsdhowto.com/Login-Class-HOWTO.txt>

<http://www.eduunix.ccut.edu.cn/index/html/unix/Absolute.OpenBSD.UNIX.For.The.Practical.Paranoid.eBook-LiB/8014final/LiB0079.html>

Dodajte nastavak **-cur** ako hoćete neku trenutnu vrednost koju može korisnik da promeni na primer

:parametar-cur=vrednost:\

Dodajte nastavak **-max** ako hoćete neku stalnu maksimalnu vrednost koju ne može korisnik da promeni na primer

:parametar-max=vrednost:\

Sistem ne čita normalno /etc/login.conf već /etc/login.conf.db, posle promena morate napraviti ponovo tu fajlu sa i onda se ponovo ulogovati da bi se to očitalo

### **cap\_mkdb /etc/login.conf**

Pogledajte kako da ograničite upotrebu memorije.

#### Za BSD i GNU/Linux

Da vidite aktuelne limite

```
ulimit -a
```

```
ulimit -aH
```

```
ulimit -aS
```

#### Za GNU/Linux

Isto možete da postignete ako ne koristite PAM sa komandama

<http://linux.die.net/man/1/ulimit>

<http://ss64.com/bash/ulimit.html>

To možete sve da podesite sa skriptom, koja se zove pomoću /etc/local.d/local.start

```
/home/bin/ulimit-
```

Da ograničite broj procesa koji mogu da se otvore, na primer

```
ulimit -Su 150
```

```
ulimit -Hu 250
```

Da ograničite broj fajli koje mogu da se otvore, na primer

```
ulimit -Sn 14000
```

```
ulimit -Hn 16000
```

## Ako neko ima fizički pristup Vašem kompjuteru

Kako da se zaštite u tom slučaju.

<http://www.cromwell-intl.com/unix/linux-break-in-howto.html>

Normalno ovo ne trebate ako samo Vi imate pristup Vašem kompjuteru, ali nikad niste potpuno sigurni da niko nema pristup njemu zar ne?

## Šta se dešava ako hackeru ukradete kompjuter

### Prey

Prey lets you keep track of your phone or laptop at all times, and will help you find it if it ever gets lost or stolen. It's lightweight, [OpenSource](#) software, and free for anyone to use. And it just works.

<http://preyproject.com/>

Instališe se ručno.

<http://www.youtube.com/watch?v=U4oB28ksilo>

<http://www.pcpress.info/hardver/racunari/otkriven-ukradeni-laptop-posle-londonskih-nemira/>

## FreeBSD Kernel i GNU/Linux Kernel nisu uvek sigurni

### IPsec

[http://www.phoronix.com/scan.php?page=news\\_item&px=ODkxMw](http://www.phoronix.com/scan.php?page=news_item&px=ODkxMw)

<http://permalink.gmane.org/gmane.os.openbsd.tech/22557>

<http://permalink.gmane.org/gmane.comp.security.bugtraq/45620>

<http://www.ns-linux.org/Vesti/da-li-je-fbi-finansirao-ipsec-stack-backdoor-u-openbsd-u>

[http://www.theregister.co.uk/2010/12/15/openbsd\\_backdoor\\_claim/](http://www.theregister.co.uk/2010/12/15/openbsd_backdoor_claim/)

[http://www.newsfactor.com/story.xhtml?story\\_id=010000L6J9PU](http://www.newsfactor.com/story.xhtml?story_id=010000L6J9PU)

Upad na stranicu

<http://linux-foundation.org/weblogs/lwf/2011/08/31/the-cracking-of-kernelorg/>

<https://lwn.net/Articles/457142/>

<http://linux.slashdot.org/story/11/08/31/2321232/Kernelorg-Compromised>

<https://www.linux.com/news/featured-blogs/171-jonathan-corbet/491001-the-cracking-of-kernelorg>

<http://www.thehackernews.com/2011/09/kernelorg-server-rooted-and-448-users.html>

<http://git-blame.blogspot.com/2011/08/how-to-inject-malicious-commit-to-git.html>

## Sistem uvek treba da bude aktuelan

Mnogo je bitno instalisati najnovije ali samo stabilne pakete u kojima su ispravljene greške.

Preko kojih je mogao napadač eventualno da dobije root pristup.

Na primer za moju Distribuciju postoji Gentoo GLSA, to je jedna lista koja navodi sve poznate propuste programa.

<http://www.gentoo.org/security/en/glsa/>

Linux Compatible vodi između ostalih novosti i listu poznatih propusta u programima pojedinih glavnih Distribucija.

<http://www.linuxcompatible.org/>

U Gentoo-u komanda

```
glsa-check -f affected
```

proverava koje sve greške postoje u instalanim programima, i ako ih ima pokušava da instalise update.

To se kod mene izvršava automatski svaki dan. Verovatno i druge Distribucije imaju nešto slično.

## Zaštitite prepisku svake vrste preko Interneta

Treba na primer zaštiti sa GnuPG elektronsku poštu i sa GnuPG ili OTR Instant Messaging

Što da drugi znaju šta Vi pišete?

[http://www.gpg4win.org/handbuecher/durchblicker\\_4.html](http://www.gpg4win.org/handbuecher/durchblicker_4.html)

## **Postavite zaštitni zid**

**Napadači ne znaju baš uvek da li se koristi smopu!M ili BSD ili GNU/Linux.**

**Oni jednostavno skeniraju statičke i dinamičke IP adrese po svim poznatim Port-ovima.**

**Pa šta nađu otvoreno...**

**Sa BSD-om i GNU/Linux-om je sigurnije plaćati preko Interneta, nego preko smopu!M-a, ali se mora paziti kako i sa kojim sistemima zaštite se štite na primer broj ugovora, korisnik, šifre i cela komunikacija.**

**A to je manje više isto i na BSD-u, GNU/Linux-u i na smopu!M-u, jer to Banka ili finansijski institut određuje. Transakcije se većinom obavljaju preko https ili Java protokola. Ima i Keylogger-a.**

**Zaštita operativnog sistema je mnogo sigurnija i lakša u BSD-u i GNU/Linux-u nego u smopu!M-u.**

**Nije na odmet pre i posle transakcije ugasiti pa ponovo upaliti softwerski ili hardwerski modem, da bi se promenila IP adresa.**

**Dobar zaštitni zid je obavezan.**

Relativna sigurnost u BSD-u i GNU/Linux-u

Šifre moraju biti veoma jake

Ključevi moraju biti jedinstveni

Nigde ne ostavljajte svoje lične podatke, jer Internet sve pamti

Kako paketi putuju po Internet mreži

Društvene mreže

Bruce Schneier

Replay attacks

Virusa ima i za BSD i GNU/Linux

Zlonamerne skripte

Fork bomb

Ako neko ima fizički pristup Vašem kompjuteru

Šta se dešava ako hackeru ukradete kompjuter

Prey

FreeBSD Kernel i GNU/Linux Kernel nisu uvek sigurni

Sistem uvek treba da bude aktuelan

Zaštitite prepisku svake vrste preko Interneta

Postavite zaštitni zid

Na početak

## **Zaštita od nepoželjnih logovanja, to jest napada na Vaš sistem**

Ima više načina za to

### **TCP-Wrappers**

**Zaštitu treba staviti na sam početak svih protokola.**

<ftp://ftp.porcupine.org/pub/security/index.html>

Za [BSD](#)

```
cd /usr/ports/security ; ls | grep tcpwrap
```

[TCP-Wrappers](#) se nalazi u [FreeBSD Base paketima](#).

Dodaci za [TCP-Wrappers](#)

```
portmaster -n security/pecl-tcpwrap
```

```
portmaster -n security/ruby-tcpwrap
```

Za [GNU/Linux](#)

```
emerge -a tcp-wrappers
```

[http://docs.redhat.com/docs/en-US/Red\\_Hat\\_Enterprise\\_Linux/3/html/Reference\\_Guide/s1-tcpwrappers-access.html](http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/3/html/Reference_Guide/s1-tcpwrappers-access.html)

Za [BSD](#)

Postoji samo

```
/etc/hosts.allow
```

## Za GNU/Linux

Prvo se izvršavaju pravila iz

```
/etc/hosts.allow
```

normalno ako je tu nešto dozvoljeno onda se pušta prolaz.

Ako se ne nađe pravilo koje nešto dozvoljava onda se gledaju dalja pravila u

```
/etc/hosts.deny
```

Normalno u fajlama se gledaju pravila odozgo na dole.

Dozvolite samo željenim adresama da mogu ulogovati preko raznih protokola.

Pažnja, samo ako sve generalno zabranite u /etc/hosts.deny, što je normalan postupak.

Onda su zabranjeni svi protokoli i sve adrese.

Neki će reći da je to paranoično, ali sigurno je sigurno.

Ako tako uradite u Vaš kompjuter može uči samo onaj kome izričito ovde date pristup, to jest dozvolite adresu i protokol koji druga strana koristi.

```
/etc/hosts.allow
```

Možete blokirati određene stanice

```
/etc/hosts
```

```
# Block a domain  
#127.0.0.1 domain
```

**Neće da radi blokiranje određenih stranica ako koristite sakrivanje IP adrese, dakle vidite dokle se ide u kontrolisanju i logovanju svega.**

## **Već rečeno, ali najbolje je da sve protokole i adrese zabranite u ovoj fajli**

Desilo mi se jedanput da adresa nije bila dozvoljena a uspela je da se uloguje!

U /etc/hosts.deny je bila opcija

sshd: UNKNOWN

Znači svi koji su poznati **KNOWN** biće dozvoljeni ili ne zabranjeni.

Jer ja nisam imao nikakve napade i nisam bio stavio generalnu zabranu.

Ta osoba je već ulazila kod mene preko statične adrese, znala je korisnika i šifru, jer mi je dobro poznata.

Odjedanput sam video u logovima da se neko ulogovao sa potpuno nepoznatom dinamičkom adresom, ali ispravno sa tačnim korisnikom i šifrom.

Šta da kažem to je bio težak udarac za mene, za svakog ko optimira svoj [GNU/Linux](#) to je...

Kontaktirao sam ga i rekao mi je da je njegov Provajder nešto promenio u svojoj konfiguraciji.

Da bih u budućnosti sprečio takva neugodna iznenadenja, odmah sam sve generalno zabranio i u hosts.allow dozvolio tu adresu sa objašnjenjem ko je to.

/etc/hosts.deny

Možete određene stranice da blokirate

[http://how-to.wikia.com/wiki/How\\_to\\_block\\_webpages\\_and\\_domain\\_using\\_the\\_hosts\\_file](http://how-to.wikia.com/wiki/How_to_block_webpages_and_domain_using_the_hosts_file)

/etc/hosts

```
...
# Block a domain
# Block a domain
#127.0.0.1 domain
127.0.0.1 www.facebook.com
127.0.0.1 www.google-analytics.com
...
```

## **Tcpcrypt**

Is a protocol that attempts to encrypt (almost) all of your network traffic. Unlike other security mechanisms, [Tpcrypt](#) works out of the box: it requires no configuration, no changes to applications, and your network connections will continue to work even if the remote end does not support [Tpcrypt](#), in which case connections will gracefully fall back to standard clear-text TCP. Install [Tpcrypt](#) and you'll feel no difference in your every day user experience, but yet your traffic will be more secure and you'll have made life much harder for hackers.

<http://tcpcrypt.org/>

<https://en.wikipedia.org/wiki/Tpcrypt>

<https://github.com/sorbo/tpcrypt>

[Instališe se ručno.](#)

Veoma je eksperimentalno, ali može da bude dobro ako se dalje razvija, zato pazite šta radite.

Možete skinuti sa ovom skriptom

/home/bin/git/git-Tpcrypt

Možete instalisati sa ovom skriptom

/home/bin/install-tpcrypt

[Zaštita od nepoželjnih logovanja, to jest napada na Vaš sistem](#)

[TCP-Wrappers](#)

[Tpcrypt](#)

[Kako zaštитити DNS](#)

[Dodatni programi за спречавање nepoželjnih логовања](#)

[На почетак](#)

## **Kako zaštитити DNS**

<http://www.dmoz.org/Computers/Internet/Protocols/DNS/>

[https://en.wikipedia.org/wiki/Domain\\_Name\\_System](https://en.wikipedia.org/wiki/Domain_Name_System)

## Razni projekti

<http://www.ccc.de/censorship/dns-howto/>

<http://www.ungefiltert-surfen.de/nameserver/>

<http://www.opennicproject.org/>

<http://www.dnssec.net/>

<https://www.iana.org/dnssec/>

[https://en.wikipedia.org/wiki/Domain\\_Name\\_System\\_Security\\_Extensions](https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions)

Takođe imate u [primerima](#) /etc/resolv.conf

Pogledajte [Dinamička adresa vidljiva na Internetu.](#)

Možete proveriti da li koristite [DNSSEC](#)

<http://test.dnssec-or-not.org/>

## OpenDNSSEC

Was created as an [OpenSource](#) turn-key solution for [DNSSEC](#). It secures zone data just before it is published in an authoritative name server.

<http://www.opendnssec.org/>

Za [BSD](#)

```
portmaster -n dns/opendnssec
```

Za [GNU/Linux](#)

```
emerge -a opendnssec
```

```
man opendnssec
```

## Unbound

is designed as a set of modular components, so that also [DNSSEC](#) (secure DNS) validation

and stub-resolvers (that do not run as a server, but are linked into an application) are easily possible.

<https://unbound.net/>

Postoji kao [PfSense paket](#).

Za [BSD](#)

```
portmaster -n dns/unbound
```

Za [GNU/Linux](#)

```
emerge -a unbound
```

## P2P DNS

Would consist of servers running caches to keep track of domain and nameserver records. Cache servers can be created with any server that supports XML-RPC or SOAP. MySQL is used to store the cache data.

<http://sourceforge.net/projects/dotp2p/>

## **Dodatni programi za sprečavanje nepoželjnih logovanja**

**Veliko je pitanje da li ovi programi mogu efikasno da zaštite Vaš sistem.**

**Dobro proučite ovu stranicu**

<http://www.ossec.net/en/attacking-loganalysis.html>

Šta se dešava ako napadač hoće da sakrije svoj Identitet i da ovu komandu za ssh?

```
ssh "myfakeuser from 10.1.1.1 port 123 ssh2"@192.168.5.1
```

Ako imate [pfSense](#) možete koristiti [pfBlocker](#), tako štitite dodatno sve Vaše kompjutere.

Ne koristite više programa, već koristite šta Vam odgovara ali ga dobro podesite.

Preporučujem [Deny Hosts](#), kod mene se odlično pokazao.

Mada ja nisam imao još napada. To jeste nisam ih primetio, niti se bilo šta čudno dešavalo.

## Deny Hosts

A utility to help sys admins thwart ssh hackers

<http://www.denyhosts.net>

<http://denyhosts.sourceforge.net/>

Za [BSD](#)

```
portmaster -n security/denyhosts
```

Za [GNU/Linux](#)

```
emerge -a app-admin/denyhosts
```

Podesite konfiguraciju

Za [BSD](#)

```
/usr/local/etc/denyhosts.conf
```

Za [GNU/Linux](#)

```
/etc/denyhosts.conf
```

Podignite servis

```
/usr/local/etc/rc.d/denyhosts start
```

Za [GNU/Linux](#)

```
/etc/init.d/denyhosts start
```

Da se stalno podiže pri dizanju sistema

## Za BSD

Za FreeBSD da se stalno podigne i da ima bolju kontrolu stavite u [/etc/rc.conf](#)

```
...  
denyhosts_enable="YES"  
syslogd_flags="-c"  
...
```

## Za GNU/Linux

```
rc-update add denyhosts default
```

Ako Deamon ne radi dobro možete staviti da se izvršava preko [Cron pravila](#).

## **psad**

Port Scanning Attack Detection daemon

Incorporates many signatures from the [Snort](#) intrusion detection system to detect probes for various backdoor programs (e.g. EvilFTP, Girlfriend, SubSeven), DDoS tools (mstream, shaft), and advanced port scans (FIN, NULL, XMAS) which are easily leveraged against a machine via [Nmap](#).

<http://www.cipherdyne.org/psad/>

## Za GNU/Linux

```
emerge -a psad
```

<http://www.cipherdyne.org/psad/docs/config.html>

Podignite ga

```
/etc/init.d/psad start
```

Da se uvek podigne pri dizanju sistema

```
rc-update add psad default
```

## Fail2ban

Scans log files like /var/log/pwdfail or /var/log/apache/error\_log and bans IP that makes too many password failures. It updates firewall rules to reject the IP address.

Radi sa zaštitnim zidovima i dosta programa. Banuje za određeno vreme adrese sa kojih su došli neuspeli logini.

[www.fail2ban.org/](http://www.fail2ban.org/)

Za [BSD](#)

```
portmaster -n security/py-fail2ban
```

Za [GNU/Linux](#)

```
emerge -a fail2ban
```

Podesite konfiguraciju

Za [BSD](#)

```
/usr/local/etc/fail2ban/
```

Za [GNU/Linux](#)

```
/etc/fail2ban/jail.conf
```

Podignite ga sa

Za [BSD](#)

```
/usr/local/etc/rc.d/fail2ban start
```

Za [GNU/Linux](#)

```
/etc/init.d/fail2ban start
```

Da se uvek starta pri podizanju sistema

Za [BSD](#)

[/etc/rc.conf](#)

```
fail2ban_enable="YES"
```

Za [GNU/Linux](#)

```
rc-update add fail2ban default
```

## PortSentry

Is part of the Abacus Project suite of security tools. It is a program designed to detect and respond to port scans against a target host in real-time. There are other port scan detectors that perform similar detection of scans, but [PortSentry](#) has some unique features that may make it worth looking into.

<http://sourceforge.net/projects/sentrytools/>

Za [BSD](#)

```
portmaster -n security/portsentry
```

Za [GNU/Linux](#)

```
emerge -a portsentry
```

## SSHGuard

Monitors services from their logging activity. It reacts to messages about dangerous activity by blocking the source address with the local firewall.

Sshguard employs a clever parser that can recognize several logging formats at once transparently (syslog, syslog-ng, metalog, multilog, raw messages), and detects attacks for many services out of the box, including SSH, FreeBSD's ftpd and dovecot. It can operate all the major firewalling systems, including [PF](#), [netfilter/iptables](#), [IPFIREWALL/ipfw](#), [IPFILTER](#).

Brani od SSH, FTP... napada, pravi pravila, tako bi trebalo, ali nije to baš tako jednostavno ni pouzdano.

<http://sshguard.sourceforge.net/>

Za [BSD](#)

```
portmaster -n security/sshguard
```

Za [GNU/Linux](#)

```
emerge -a sshguard
```

Za mene ide suviše u dubinu, nema neke koristi i teško se podešava.

Probao sam ga, radio je nekoliko meseci, video da drugi programi bolje rade i sva podešavanja izbrisao i deinstalisao ga.

Napravite Whitelist

```
cp -a /usr/share/doc/sshguard-verzija/whitelistfile.example /etc/sshguard.friends
```

Podesite je prema vašim prijateljima, kojima hoćete da dozvolite pristup

To je ako hoćete da startate ručno sa

```
sshguard -w /etc/sshguard.friends
```

Podesite prema

<http://ns-linux.org/Uputstva/Opste/odbijanje-ssh-napada>

Za početak, treba da dodate novi lanac u iptables:

```
iptables -N sshguard
```

```
iptables -A INPUT -p tcp --dport 22 -j sshguard
```

Da bi konfiguracija bila zapamćena, ili stavite ove dve komande u neku boot skriptu ili, ako imate init skriptu koja to radi, sačuvajte setovanja sa:

```
/etc/init.d/iptables save
```

Naravno, kod Vas skripta može biti na drugom mestu. Meni je ta skripta u /etc/rc.firewall  
Drugi korak je da podesite /etc/syslog-ng/syslog-ng.conf.

Nakon ovoga, resetujte syslog-ng i trebali biste da dobijete fajl /var/log/ssh.log u kome će se nalaziti svi pristupi Vašoj mašini preko SSH, kao i akcije koje je sshguard preduzeo.

```
/etc/init.d/rc.firewall restart
```

```
/etc/init.d/syslog-ng restart
```

[Zaštita od nepoželjnih logovanja, to jest napada na Vaš sistem](#)

[TCP-Wrappers](#)

[Tcpcrypt](#)

[Kako zaštititi DNS](#)

[Dodatni programi za sprečavanje nepoželjnih logovanja](#)

[Deny Hosts](#)

[Fail2ban](#)

[PortSentry](#)

[SSHGuard](#)

[Na početak](#)

## **Zaštitni zid, Firewall**

**Zaštitni zid ili Firewall je dobar samo ukoliko ga dobro i stalno održavate da je na najvišem mogućem nivou zaštite.**

[https://en.wikipedia.org/wiki/Personal\\_firewall](https://en.wikipedia.org/wiki/Personal_firewall)

[https://en.wikipedia.org/wiki/Comparison\\_of\\_firewalls](https://en.wikipedia.org/wiki/Comparison_of_firewalls)

## **Zaštitni zid, Firewall za BSD**

Pogledajte [Router](#), posebno [pfSense](#), koja koristi [PF](#).

<http://www.freebsd.org/doc/handbook/firewalls.html>

## **PF, The OpenBSD Packet Filter**

Originalno je iz [OpenBSD](#)-a, znači zaostaju verzije u [FreeBSD](#)-u i ostalim [BSD](#) Distribucijama.

Možete podešavati [PF](#) grafički sa [FW Builder](#) ili osnovno sa [PF Firewall Manager](#). [PF je Firewall koji se koristi u pfSense](#).

<http://www.openbsd.org/faq/pf/>

<http://www.freebsd.org/doc/handbook/firewalls-pf.html>

<http://www.freebsd.org/doc/en/books/handbook/firewalls-pf.html>

<http://pf4freebsd.love2party.net/>

<http://www.netbsd.org/docs/network/pf.html>

[https://calomel.org/pf\\_config.html](https://calomel.org/pf_config.html)

<http://home.nuug.no/~peter/pf/>

<http://www.benzedrine.cx/pf.html>

<http://undeadly.org/cgi?action=article&sid=20060927091645>

<http://www.cyberciti.biz/faq/opebsd-pf-firewall-block-subnets-ip-address/>

<http://gala4th.blogspot.com/2010/12/set-up-pf-packet-filter-on-freebsd.html>

<https://sites.google.com/site/clickdeathsquad/Home/cds-bsdfirewall>

<http://www.lerota.net/linuxunix/freebsd-router-firewall-howto/>

[https://en.wikipedia.org/wiki/PF\\_%28firewall%29](https://en.wikipedia.org/wiki/PF_%28firewall%29)

Kanal #pf na [Freenode](#) povezan sa

[http://www.probsd.net/pf/index.php/Main\\_Page](http://www.probsd.net/pf/index.php/Main_Page)

Email lista za [PF](#) u [FreeBSD](#)

<http://lists.freebsd.org/mailman/listinfo/freebsd-pf>

Problem sa novim kodom

<http://bsdly.blogspot.de/2011/07/anticipating-post-altq-world.html>

Izgleda da Apple neće da vraća nazad kod u [PF](#), ali to je u skladu sa [BSD licencom](#).

<http://callfortesting.org/macpf/>

[BSD Magazine](#) je u sledećim izdanjima opisao [PF](#)

01.2008,

Imate primere u

```
cd /usr/share/examples/pf ; ls
```

Treba da podesite CUSTOM [FreeBSD Kernel](#) za [PF](#)

```
man pf.conf
```

```
# PF, The OpenBSD Packet Filter
device      pf          # packet filter, man pf
device      pflog       # packet filter logging interface, man pflog
device      pfsync      # packet filter state table logging interface, man pfsync
```

Treba da podesite CUSTOM [FreeBSD Kernel](#) za ALTQ

```
man altq
```

<http://www.freebsd.org/cgi/man.cgi?query=pf.conf&sektion=5#QUEUEING%2fALTQ>

```
# ALTQ Support for PF, The OpenBSD Packet Filter
# man altq
options      ALTQ
options      ALTQ_CBQ      # Class Bases Queuing (CBQ)
options      ALTQ_RED      # Random Early Detection (RED)
options      ALTQ_RIO      # RED In/Out
options      ALTQ_HFSC     # Hierarchical Packet Scheduler (HFSC)
options      ALTQ_PRIQ     # Priority Queuing (PRIQ)
options      ALTQ_NOPCC    # Required for SMP build
```

Da se uvek starta pri podizanju sistema

[/etc/rc.conf](#)

```
# Enable the PF, The OpenBSD Packet Filter Firewall
pf_rules="/etc/pf.conf"
```

```
pf_enable="YES"
pf_flags=""
pflog_enable="YES"
```

Konfiguracija je u

```
/etc/pf.conf
```

Pravila su zapamćena u privremenoj fajli

```
cat /tmp/rules.debug
```

Podešava se sa

```
man pfctl
```

```
pfctl -h
```

Provera da li je /etc/pf.conf u redu

```
pfctl -n
```

```
pfctl -nf /etc/pf.conf
```

Isto proverava, ali daje i izveštaj

```
pfctl -v nf /etc/pf.conf
```

Uključuje [PF](#)

```
pfctl -e
```

Isključuje [PF](#)

```
pfctl -d
```

Ponovo pokreće [PF](#) i učitava iz konfiguracije

```
pfctl -F all -f /etc/pf.conf
```

Pokazuje sva Vaša [PF](#) pravila

```
pfctl -v -s rules
```

```
pfctl -sa
```

pfTop

Pokazuje šta se dešava, slično kao [top](#)

```
pftop
```

Pokazuje stanje

```
pfctl -v -s state
```

Prikazuje ulazne veze

```
pfctl -ss
```

Prikazuje po konekciji

```
pfctl -si
```

Prikazuje limite

```
pfctl -sm
```

Možete koristiti [tcpdump](#) da kontrolišete šta se dešava

```
tcpdump -e -i pflog0
```

*Kraj PF, The OpenBSD Packet Filter*

## IPFW, The IPFIREWALL

<http://www.freebsd.org/doc/handbook/firewalls-ipfw.html>

[http://www.freebsdwiki.net/index.php/Firewall,\\_Configuring](http://www.freebsdwiki.net/index.php/Firewall,_Configuring)

<http://www.freebsddiary.org/ipfw.php>

<http://www.cyberciti.biz/faq/howto-setup-freebsd-ipfw-firewall/>

<http://www.rasyid.net/2007/11/18/101-freebsd-ipfw-resources/>

<https://en.wikipedia.org/wiki/Ipfirewall>

Originalno je iz [FreeBSD](#)-a.

Treba da podesite [FreeBSD Kernel](#).

```
man 4 ipfw
```

```
man 8 ipfw
```

```
man dumynet
```

```
less /usr/src/sys/netinet/ipfw/dumynet.txt
```

Primarno se koriste

```
/etc/rc.firewall
```

ili

```
/etc/rc.firewall6
```

Da se podigne modul za [IPFW](#)

[/boot/loader.conf](#)

```
ipfw_load="YES"
```

Da se uvek starta pri podizanju sistema

[/etc/rc.conf](#)

```
# Enable IPFW, The IPFIREWALL, FreeBSD Firewall  
firewall_enable="YES"  
firewall_type="type"
```

type može biti

Propušta sve

```
"open"
```

Štiti samo ovu mašinu

```
"client"
```

Štiti celu mrežu

```
"simple"
```

Zabranjuje ceo protok, sem lokalne mreže

```
"closed"
```

Brani da se izvrše pravila zaštitnog zida

```
"UNKNOWN"
```

Apsolutna adresa fajle koja sadrži pravila zaštitnog zida

```
"filename"
```

Da vidite šta ima

```
find /usr/ports/* | grep ipfw
```

## IPFW grapher

Displays a graphical overview of bytes going through your [IPFW](#) rules and a piled overview of the percentage on which rule it passed.

<http://www.mavetju.org/networking/tools.php>

```
portmaster -n net/ipfw-graph
```

## IPA\_IPFW

Accounting module for [FreeBSD IP Firewall](#)

[http://ipa-system.sourceforge.net/modules/ipa\\_ipfw/](http://ipa-system.sourceforge.net/modules/ipa_ipfw/)

```
portmaster -n net/ipa_ipfw
```

*Kraj IPFW, The IPFIREWALL*

## IPF, IP Filter

Originalno je iz [NetBSD](#)-a, znači zaostaju verzije sa originalnim verzjama.

<http://www.freebsd.org/doc/handbook/firewalls-ipf.html>

<http://www.phildev.net/ipf/index.html>

<https://en.wikipedia.org/wiki/IPFilter>

Treba da podesite [FreeBSD Kernel](#).

Da se uvek starta pri podizanju sistema

[/etc/rc.conf](#)

```
# Enable IPF, IP Filter  
ipfilter_enable="YES"
```

[Na početak](#)

## **Zaštitni zid, Firewall za GNU/Linux**

**Prvi Firewall za GNU/Linux je bio ipfwadm kojem je bio uzor IPFW.**

**GNU/Linux Kernel ima odličan zaštitni zid, a to je IPtables / Netfilter**

**U konfiguraciji GNU/Linux Kernel-a sve opcije uključiti pod**

**Networking / Networking options / Network packet filtering framework (Netfilter)**

**Nije verovatno sve potrebno, ali tu od viška glava ne boli.**

## **Iptables / Netfilter**

Linux kernel (2.4+) firewall, NAT and packet mangling tools

Osnova za zaštitni zid, dodatak na **GNU/Linux Kernel**-ov Firewall

Sve na tim stranicama dobro proučite, dobro razumite šta sve piše, to je obavezna lektira.

<http://www.netfilter.org/>  
<http://www.iptables.org/>

<http://netfilter.org/documentation/>

**emerge -a iptables libnetfilter\_conntrack libnetfilter\_log conntrack-tools**

<http://security.maruhn.com/>

<https://help.ubuntu.com/community/IptablesHowTo>

[https://wiki.archlinux.org/index.php/Simple\\_stateful\\_firewall\\_HOWTO](https://wiki.archlinux.org/index.php/Simple_stateful_firewall_HOWTO)

## Xtables-addons

A set of NetFilter's modules, that not included in main tree

Xtables-addons is the successor to patch-o-matic(-ng)

Zamenjuje patch-o-matic, ne treba se više [GNU/Linux Kernel](#) pačovati

<http://xtables-addons.sourceforge.net/>

```
emerge -a xtables-addons
```

```
man xtables-addons
```

Sadrži geoip i TARPIT modul pored ostalih koje sam pre besupešno pokušavao da instaliram.

Možete na primer dodati komandu u

/etc/rc-firewall/rc.firewall

```
...  
$IPTABLES -A INPUT -p tcp --dport $SSH_PORT -m geoip --src-cc BA,CH,HR,RS \  
      -state --syn --state NEW \  
      -m limit --limit 1/minute --limit-burst 1 -j ACCEPT  
...
```

kojom dozvoljavate samo logovanje iz Bosne, Švajcarske, Hrvatske i Srbije primere imate na

<http://people.netfilter.org/peejix/geoip/howto/geoip-HOWTO-3.html>

Pogledajte [Da bi to mogli koristiti GeoIP za Firewall i kontrolu.](#)

## IPsets

IPset tool for iptables, successor to ippool

<http://ipset.netfilter.org/>

```
emerge -a ipset
```

Ako Vam treba Bridging

## **bridge**

<http://bridge.sourceforge.net/>

<http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge>

```
emerge -a bridge-utils
```

## **ebtables**

Povezuje Bridging i iptables / netfilter

Utility that enables basic Ethernet frame filtering on a Linux bridge, MAC NAT and brouting

<http://ebtables.sourceforge.net/>

```
emerge -a ebtables
```

Da vidite šta sve postoji u bazi programa

```
eix -S firewall
```

```
eix -S ethernet
```

## **GUI za Firewall**

### **GUI su samo šminka, prava snaga BSD i GNU/Linux-a je konzola**

Ali u njih ne treba biti siguran, prave pravila za zaštitini zid, izvršavaju ih automatski (ako se namesti). Meni se dešavalo da su Port-ovi bili zatvoreni iako sam ih u GUI-u otvorio.

I ja sam zbog lakoće prvo koristio razne GUI-e, pa sam imao razne neobjasnjive greške.

Kao Port je otvoren ali ne može se ostvariti konekcija...

Onda sam zasukao rukave i od tada u [GNU/Linux](#)-u koristim samo moj zaštitni zid a [GUI](#) su eventualno tu samo za informaciju koji servisi koriste koje portove, mada i tu lažu.

Više nemam nijedan [GUI](#) u [GNU/Linux](#)-u, sve radim ručno i sve je kako ja hoću i nemam nijedan napad otkad koristim svoj zaštitni zid. Ali se ne uljuljkujem u sigurnost, već stalno posmatram i dopunjujem moj zaštitni zid, ako se nađe potreba, što je retko.

Koristio sam 3 godine Guarddog, probao sam Shorewall, KmyFirewall.

Postoje razni [GUI](#) i konzolni programi za zaštitni zid kao

## FW Builder

Consists of object-oriented GUI and set of policy compilers for various firewall platforms. In Firewall Builder, firewall policy is a set of rules, each rule consists of abstract objects which represent real network objects and services (hosts, routers, firewalls, networks, protocols). Firewall Builder helps user maintain database of objects and allows policy editing using simple drag-and-drop operations.

<http://www/fwbuilder.org/>

<http://sourceforge.net/projects/fwbuilder/>

Za [BSD](#)

portmaster -n security/fwbuilder-verzija

Za [GNU/Linux](#)

emerge -a fwbuilder

fwbuilder -h

man fwbuilder

Video uputstvo kako se koristi [FW Builder](#)

[http://www/fwbuilder.org/4.0/videos.html?utm\\_source=app&utm\\_medium=dialog&utm\\_campaign=quick\\_start](http://www/fwbuilder.org/4.0/videos.html?utm_source=app&utm_medium=dialog&utm_campaign=quick_start)  
[https://www.youtube.com/v/Q5GPrkwyGxw?fs=1&hl=en\\_US](https://www.youtube.com/v/Q5GPrkwyGxw?fs=1&hl=en_US)

## **Qtfw**

Is a Qt gui frontend for [IPFW](#) utility in [FreeBSD](#). It helps configuring firewall in [FreeBSD](#) with a niceand comprehensive user interface.

Ne razvija se više.

<http://sourceforge.net/projects/qtfw/>

Za [BSD](#)

portmaster -n security/qtfw

Samo za [GNU/Linux](#)

Guarddog

<http://www.simonzone.com/software/guarddog/>

KMyFirewall

<http://www.kmyfirewall.org/>

Shorewall

<http://www.shorewall.net/>

Firestarter

<http://www.fs-security.com/>

I mnogo drugih...

## **Koja aplikacija koji Port normalno koristi**

[https://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

<http://www.chebucto.ns.ca/~rakerman/port-table.html>

[http://www.practicallynetworked.com/sharing/app\\_port\\_list.htm](http://www.practicallynetworked.com/sharing/app_port_list.htm)

<http://andrew.triumf.ca/ports/other.html>

**A ovde vidite kojoj aplikaciji je neki Port dodeljen, to jest imate upit.**

<http://andrew.triumf.ca/cgi-bin/port>

<http://www.portsdb.org.uk/>

<http://www.canyouseeme.org/>

## Kako da neki Port propustite

**Sigurno želite da se povežete sa nekim preko SSH, SSHFS, Rsync, Distcc i drugih protokola.**

**Normalno za to morate da propustite u Vašem Modemu, Routeru određene Portove.**

**Nemojte koristiti nijedan Port a da ne znate za šta se on koristi i da li ima alternativa, to jest da li se može program podešiti na neki drugi Port. Mnogi programi to dozvoljavaju, pa koristite to onda, da bi bili sigurniji.**

**Koristite ako možete samo Port-ove za Vaše programe iz ovog opsega**

**Dynamic and/or private ports: 49152-65535.**

<http://portforward.com/>

[https://en.wikipedia.org/wiki/Port\\_forwarding](https://en.wikipedia.org/wiki/Port_forwarding)

<http://www.wikihow.com/Set-up-Port-Forwarding-on-a-Router>

## **Neki Port niste otvorili, ali ih neki Program otvara**

Na primer Psi otvara Port 8010, ako je samo upisan u njemu i ako je pokrenut.

Znači upisati u programima Port-ove tek kad Vam trebaju i uvek kontrolisati šta je otvoreno.

## **Precizno podešavanje zaštitnog zida preko GUI-a nije moguće**

GUI nemaju sve te opcije koje mogu da se dodaju.

Meni je u mojoj skripti i napisano odakle to imam, pa ako mi nešto nije jasno, mogu tamo da pogledam.

Imam i više rešenja u njoj za istu stvar (svako objašnjeno) pa kako mi nekad treba, veća ili manja sigurnosti i da li neki modul trenutno radi ili ne radi.

## Kako da pravite Iptables pravila

Imate dosta primera u

```
/etc/rc.firewall/rc.firewall-primer
```

<http://www.thegeekstuff.com/2011/06/iptables-rules-examples/>

## Sa zaštitnim zidom sve zabraniti

i onda restartovati zaštitni zid sa

```
/etc/rc.firewall restart
```

ili

```
firewall restart
```

Najbolje je kontrolisati se od spolja sa, nalazi skoro sve

```
nmap -v -A IP-Adress
```

Pogledajte [Kontrola](#)

Nije umetnost sve zabraniti i dozvoljavati samo ono što je potrebno. Ima tu finesa ali osnova je laka.

Ovo je tema za sebe i već je dovoljno objašnjena. Više objašnjenja u fajli

```
/etc/rc.firewall
```

```
iptables -P INPUT DROP  
iptables -P OUTPUT DROP  
iptables -P FORWARD DROP
```

Dakle sve je zabranjeno.

A Vi hoćete poslati elektronsku poštu, ne možete a u

/var/log/messages

(možda u drugim Distribucijama je neka druga fajla) piše, otprilike, da je pokušan saobraćaj na

```
SMTP 25 TCP  
SMTPS SSL 465 TCP  
POP3 110 TCP  
POP3S SSL 995 TCP  
NNTP 119 TCP
```

Port-ovima ali da je onemogućen.

**Znači propustite te Port-ove i moći ćete koristiti elektronsku poštu.  
Tako uradite za svaku aplikaciju koja Vam je potrebna.**

**Treba znati da napadači znaju koji se Port-ovi koriste za najvažnije programe.**

**Pa je poželjno za sve programe, ako to dopuštaju, da se ti Port-ovi promene u  
više vrednosti (više od 50000 na primer).**

**Menjati te Port-ove u konfiguracionim fajlama, programima, zaštitnom zidu, i  
eventuelno u zaštitnom zidu od Router-a.**

**Ne isključivati zbog jednostavnosti ili lakoće zaštitni zid od Router-a.**

**Bolje je biti duplo zaštićen, iako to zahteva malo više rada.**

U /etc/services je napisano koji programi koriste koji Port per default.  
Možete tu i dodati programe i Port-ove, samo ako mora.

**Većinom su napadi upereni na na Port 22 TCP, a to je SSH.**

**Ako to uspeju treba im još samo da probiju šifru.**

**Treba zabraniti generalno preko SSH-a root pristup na kompjuter bez SSH ključeva razume se.**

**Pogledajte SSH protokol.**

**Za ovo sve ne postoje GUI, već se mora raditi u konzoli**

**Što bude veća baza korisnika BSD i GNU/Linux-a to će biti i veća želja Hacker-a da više obrate pažnju na BSD i GNU/Linux te da i njega usreće sa više virus-a i ostalih stvari sa kojima usrećuju smopu!M korisnike.**

**Što bolja i ažurnija zaštita to je teže napadačima.**

**Prvo sve zabraniti pa onda otvarati portove to jest servise koji Vam trebaju.**

**Dobro razmislite šta Vam treba. Firewall se može dinamički menjati.**

**Ne verujte nikakvim zaštitnim zidovima koji dolaze uz Distribuciju ili nekom GUI-u.**

**Najčistije je da svako od početka nauči Iptables pravila i da zna šta njegov zaštitni zid radi. Ima toliko dobrih primera na Internetu.**

**Nije potreban nikakav program da biste promenili neko Iptables pravilo, samo konzola, Midnight Commander ili Nano.**

## **Firewall skripta /etc/rc.firewall**

Napravite direktorijum

```
mkdir /etc/rc-firewall
```

Imate primer moje firewall skripte

```
/etc/rc-firewall/rc.firewall-primer
```

Napravite linkove da biste imali u pregledu razne verzije rc.firewall fajle.

Osiguravajte pri promenama, pamtite stare verzije.

```
In -s /etc/rc.firewall /etc/rc.firewall
```

```
In -s /etc/rc.firewall /home/bin/firewall
```

Ne treba ako nemate [GUI](#)

```
In -s /etc/rc.firewall~ /etc/rc.firewall~
```

Restartujte zaštitni zid

```
/etc/init.d/firewall restart
```

ili jednostavno ako je u path-u

```
firewall restart
```

Da se svaki sat ponovo restartuje zaštitni zid, to jest da ne bude slučajno isključen duže vreme. Možete to staviti u [pravila za cron](#). Mada to ne preporučujem, isključio sam.

Tu sam imao greške da mi se svaki sat prekidala veza u [Xchat](#)-u.

A firewall je svejedno stalno podigunut. Pa sam ovo isključio.

```
/etc/cron.hourly/firewall
```

```
#!/bin/sh
```

```
exec /etc/rc.firewall restart
```

## Firewall skripta /etc/init.d/firewall

Ova skripta se starta automatski preko

```
/etc/local.d/local.start
```

/etc/init.d/firewall

## Da bi to mogli koristiti GeolP za Firewall i kontrolu

Trebate imati instalisan [GeolP](#)

Pogledajte [Xtables-addons](#)

<http://netfilter.org/projects/patch-o-matic/index.html>

base, extra i external repository

Tu ima link za GeolP Howto koji nije ispravan, pravilno je

<http://people.netfilter.org/peejix/geoip/howto/geoip-HOWTO.html>

Kako da koristite za analizu napada

[http://www.tuxj0b.de/Script\\_for\\_auth.log\\_and\\_kern.log\\_analysis](http://www.tuxj0b.de/Script_for_auth.log_and_kern.log_analysis)

Sve pročitajte i skinite na primer sa

<http://people.netfilter.org/peejix/geoip/tools>

csv2bin-20041103.tar.gz

u

/paket/Net/Sigurnost/GeoIP/Source

tu ga prevedite sa

make

i prebacite sa

mv ./csv2bin ../

Napravite potrebni direktorijum sa

SU

mkdir /var/geoip

Zaštitni zid, Firewall

Zaštitni zid, Firewall za BSD

IPFW, The IPFIREWALL

Qtfw

PF, The OpenBSD Packet Filter

IPF, IP Filter

Zaštitni zid, Firewall za GNU/Linux

Iptables / Netfilter

GUI za Firewall

Koja aplikacija koji Port normalno koristi

Kako da neki Port propustite

Neki Port niste otvorili, ali ih neki Program otvara

Precizno podešavanje zaštitnog zida preko GUI-a nije moguće

Kako da pravite Iptables pravila

Sa zaštitnim zidom sve zabraniti

Ne isključivati zbog jednostavnosti ili lakoće zaštitni zid od Router-a

Većinom su napadi upereni na na Port 22 TCP a to je SSH

Za ovo sve ne postoje GUI već se mora raditi u konzoli

Firewall skripta /etc/rc.firewall

Da bi to mogli koristiti GeolP za Firewall i kontrolu

Na početak

## **Kontrola**

**Ove i druge alate koriste napadači na sistem.**

**Zato sami proverite i ne mislite da kad jedanput ostvarite stanje sigurnosti, da Vam više niko ništa ne može!**

**Sigurnost je jedan proces koji nikada ne prestaje. Sve je dinamično.**

**Pratite stanje na sve moguće načine koji su Vam pri ruci.**

**Informacija je sve.**

**Ni napadači ne spavaju, već stalno izmišljaju nove načine kako da Vam napakoste.**

**Njima je bitna samo root-ova šifra ili neki drugi način, preko nekog exploit-a (greške nekog programa), da uđu kao administrator u sistem i onda nema više ništa od sigurnosti.**

**Tu im stavite barijeru sa jakim šiframa bolje parafrazama (rečenicama) koje samo vi znate, firewall koji stalno obnavljate, bazu programa koju**

**stalno obnavljajte.**

**To nije udobno, ali je dosta sigurno.**

**Želite li udobnost onda idete u smopu!M, a BSD i GNU/Linux su prvenstveno za sigurnost pa tek onda udobnost.**

**Kod smopu!M-a je sam sistem šupalj kao švajcarski sir, pa ne vrede nikakve nadogradnje kao na primer Zone Alarm.**

**Virusa ima i za BSD i GNU/Linux, mada se većinom koriste zlonamerne skripte (koji Vam na primer brišu sve fajle...).**

**Hakeri su u stanju da menjaju izvršne programe da prvo izvrše njihov kod pa tek onda stvarni kod programa, menjaju logove i Vi više ne možete verovati /var/log.**

**Preko Vašeg sistema napadaju druge... Zato što sigurnije to bolje...**

**Vi sigurno ne želite posetu policije što je sa Vašeg kompjutera napadnuta neka mreža, organizacija, državna ustanova, firma...**

**Posetite obavezno ove i ostale stranice koje pišu o sigurnosti**

<http://www.linuxsecurity.com>

<http://insecure.org/>

<http://sectools.org/>

<http://secunia.com/>

[http://www.linuxtopia.org/Linux\\_Security\\_HOWTO/index.html](http://www.linuxtopia.org/Linux_Security_HOWTO/index.html)

<http://www.linuxhaxor.net/2007/11/21/10-basic-linux-security-tips-to-implement/>

<http://www.heise-online.co.uk/security/How-Skype-Co-get-round-firewalls--/features/82481>

<http://www.linuxhaxor.net/2007/12/09/9-common-wireless-hacking-tools/>

[http://www.linuxquestions.org/linux/answers/Security/SSL\\_Encrypting\\_Syslog\\_via\\_Stunnel](http://www.linuxquestions.org/linux/answers/Security/SSL_Encrypting_Syslog_via_Stunnel)

[http://www.linuxquestions.org/linux/answers/Security/Advance\\_linux\\_command](http://www.linuxquestions.org/linux/answers/Security/Advance_linux_command)

[http://www.linuxquestions.org/linux/answers/Security/A\\_Couple\\_Quick\\_find\\_Tips](http://www.linuxquestions.org/linux/answers/Security/A_Couple_Quick_find_Tips)

<http://rimuhosting.com/howto/ports.jsp>

<http://www.fiercevoip.com/>

<http://www.phearless.org/>

Ova stranica je po meni odlična, nema bolje za sve informacije o sigurnosti i protokolima, obavezno pročitajte. Na nemačkom je.

Ispati se prevesti je u [nekom programu](#) ili [stranici za prevođenje](#).

**<http://hp.kairaven.de/>**

Popularna distribucija za sigurnost i hackerske napade.

Sve što ona ima, može se imati u [Gentoo](#)-u.

<http://www.remote-exploit.org/backtrack.html>

<http://www.linux.com/articles/61417>

<http://www.lugons.org/Uputstva/Opste/wep-cracking>

<http://www.elitesecurity.org/t331141-3>

<http://www.elitesecurity.org/t318978-SSH-veza-ne-moze-da-se-uspostaviti-posle-nezeljenog-reboota>

<http://www.elitesecurity.org/t335294-wireless-sigurnost-podataka>

<http://www.markomdizajn.com/blog/zbrka-sa-rezultatima-pretrage>

Meni ovo sve liči na Orvela. Sve je ovo povezano, mada se u javnosti to tako ne prikazuje. Ide se u totalitarno društvo. To je trend u celom svetu posle famoznog 11. septembra, koji su sami Amerikanci ,ili tačnije rečeno koji njima rukuju, inscenirali.

Čekajte sledeću **veštačku veliku krizu** i vidite šta će tada biti.....

**Ne preporučujem da koristite za pretraživanje Interneta [Google](#), koristite samo [Stranice za pretraživanje Interneta koje čuvaju Vašu sigurnost](#).**

**Redovno pregledajte sistemske log fajle**

**/var/log**

**/var/log/messages**

**i ostale fajle u /var/log direktorijumu**

**tail -f /var/log/messages**

## Koji programi postoje za kontrolu

Ovde imate opis o dosta programa

<http://www.ubuntu-unleashed.com/2008/06/top-security-tools-in-ubuntu.html>

Da vidite šta ima

Za [BSD](#)

```
find /usr/ports/* | grep crack
```

```
find /usr/ports/* | grep rack
```

Za [GNU/Linux](#)

```
eix rack
```

```
eix crack
```

Instališite ove programe, zlu ne trebalo. Ima ih još ali i ovo je za početak možda mnogo. Nemojte sve instalirati, već ih probajte jedan po jedan.

Pogledajte i [protok podataka prema Internetu](#).

Najvažniji su [Bind Tools](#), [DJBDNS](#), [whois](#), [Host](#), [Nmap](#).

### Bind Tools

The user space command line tools from the latest version of BIND: dig, host, and nslookup, dnssec-keygen

<https://www.isc.org/software/bind>

Za [BSD](#)

[Bind Tools](#) se nalaze u [FreeBSD Base paketima](#).

ICS Bind Tools

```
portmaster -n dns/bind-tools
```

Za [GNU/Linux](#)

```
emerge -a net-dns/bind-tools
```

## DJBDNS

Is a collection of Domain Name System tools.

<http://cr.yp.to/djbdns.html>

<http://tinydns.org/>

```
portmaster -n dns/djbdns
```

Za [GNU/Linux](#)

```
emerge -a net-dns/djbdns
```

## whois

Improved Whois Client

<http://www.linux.it/~md/software/>

Za [BSD](#)

[whois](#) se nalazi u [FreeBSD Base paketima](#).

```
portmaster -n net/whois
```

Za [GNU/Linux](#)

```
emerge -a whois
```

## Host

A powerful command-line DNS query and test tool implementing many additional protocols

<http://www.weird.com/~woods/projects/host.html>

Za [BSD](#)

[Host](#) se nalazi u [FreeBSD Base paketima](#).

Za [GNU/Linux](#)

```
emerge -a net-dns/host
```

## Nmap

A utility for network exploration or security auditing

Is a utility for network exploration and security auditing. It supports various types of host discovery (determine which hosts are up), many port scanning techniques for different protocols, version detection (determine service protocols and application versions listening behind ports), and TCP/IP stack fingerprinting (remote host OS or device identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and much more.

<http://nmap.org>

Postoji kao [PfSense paket](#).

Za [BSD](#)

```
portmaster -n security/nmap
```

Za [GNU/Linux](#)

```
emerge -a nmap
```

## Zenmap

[Zenmap](#) is the official [GUI](#) front end for the Nmap port scanning tool. Originally based on Umit, it has replaced NmapFE as per Nmap 4.50. Also included are python based Nmap auxiliary tools (currently Ndifff).

<http://nmap.org/zenmap/>

Za [BSD](#)

Postoji [PBI](#) paket.

```
portmaster -n security/zenmap
```

Za [GNU/Linux](#)

Vec je instalisan sa [Nmap](#).

## NmapSi4

Is a complete Qt-based Gui with the design goals to provide a complete [Nmap](#) interface for Users, in order to management all options of this powerful security net scanner!

Ne radi dobro, bolje je originalni [Zenmap](#).

<http://www.nmaps4.org/>

Za [BSD](#)

```
portmaster -n security/nmappsi4
```

Za [GNU/Linux](#)

```
emerge -a net-analyzer/nmappsi
```

*Kraj Nmap*

## Netcat klonovi

<https://en.wikipedia.org/wiki/Netcat>

Da vidite šta ima

Za [BSD](#)

```
find /usr/ports/* | grep netcat
```

Za [GNU/Linux](#)

```
eix netcat
```

```
eix -S netcat
```

## Netcat

Is a simple Unix utility which reads and writes data across network connections using TCP or UDP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. At the same time it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities.

<http://nc110.sourceforge.net/>

Za [BSD](#)

[Netcat](#) se nalazi u [FreeBSD Base paketima](#).

Ako hoćete noviju verziju

```
portmaster -n net/netcat
```

Za [GNU/Linux](#)

```
emerge -a netcat
```

## GNU Netcat

Is a featured networking utility which reads and writes data across network connections, using the TCP/IP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities.

<http://netcat.sourceforge.net>

Za [BSD](#)

```
portmaster -n net/gnetcat
```

Za [GNU/Linux](#)

```
emerge -a net-analyzer/gnu-netcat
```

Ako Vam kad zatreba [Telnet](#) pristup localhost-u a nemate [Telnet](#) original, možete koristiti i [Putty](#).

Na primer za [SimpServer](#)

```
gnetcat -T localhost 10023
```

Možete napraviti hyperlink sa na primer, to nije potrebno za [BSD](#), jer ima originalni [Telnet](#)

```
In -s /usr/bin/netcat /usr/local/bin/telnet
```

## Cryptcat

Cryptcat is the standard [Netcat](#) enhanced with twofish encryption.

<http://cryptcat.sourceforge.net/>

Za [BSD](#)

```
portmaster -n net/cryptcat
```

Za [GNU/Linux](#)

```
emerge -a cryptcat
```

```
man nc
```

```
man netcat
```

```
nc --help
```

```
netcat --help
```

*kraj Netcat klonovi*

## Telnet

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

Za BSD

Telnet se nalazi u FreeBSD Base paketima.

Za GNU/Linux

Ima više verzija na primer

```
emerge -a net-misc/telnet-bsd
```

```
man telnet
```

```
telnet --help
```

## **PHRACK**

A Hacker magazine by the community, for the community...

<http://www.phrack.org/>

Za GNU/Linux

```
emerge -a app-doc/phrack-all
```

Možete čitati i na stranici, nalaze se dokumenta u

/usr/share/doc/phrack/

## **OpenVas**

A remote security scanner

<http://www.openvas.org/>

Za BSD

Ako hoćete klijenta

```
portmaster -n security/openvas-client
```

Ako hoćete server

```
portmaster -n security/openvas-server
```

Za [GNU/Linux](#)

```
emerge -a net-analyzer/openvas
```

## **Hping**

A ping like TCP/IP packet assembler/analyzer

<http://www.hping.org>

Za [BSD](#)

```
portmaster -n net/hping-verzija
```

Za [GNU/Linux](#)

```
emerge -a hping
```

## **fping**

A utility to ping multiple hosts at once

<http://fping.sourceforge.net/>

Za [BSD](#)

```
portmaster -n net/fping
```

Ako hoćete IPV6 verziju

```
portmaster -n net/fping+ipv6
```

Za [GNU/Linux](#)

```
emerge -a fping
```

## Monit

A utility for monitoring and managing daemons or similar programs running on a Unix system.

<http://mmonit.com/monit/>

Za [BSD](#)

```
portmaster -n sysutils/monit
```

Za [GNU/Linux](#)

```
emerge -a monit
```

<http://www.debianhelp.co.uk/monit.htm>

<http://foscasts.com/screencasts/6-System-Monitoring-With-Monit>

## TTCP

Tool to test TCP and UDP throughput

<http://ftp.arl.mil/~mike/ttcp.html>

Za [BSD](#)

```
portmaster -n benchmarks/ttcp
```

Za [GNU/Linux](#)

```
emerge -a net-analyzer/ttcp
```

## dsniff

A collection of tools for network auditing and penetration testing

<http://www.monkey.org/~dugsong/dsniff/>

Za BSD

```
portmaster -n security/dsniff
```

Za GNU/Linux

```
emerge -a dsniff
```

## **tcpdump**

A Tool for network monitoring and data acquisition

<http://www.tcpdump.org>

Za BSD

tcpdump se nalazi u [FreeBSD Base paketima](#).

Za GNU/Linux

```
emerge -a net-analyzer/tcpdump
```

Da vidite šta se sve dešava na Vašem Internet priključku

```
tcpdump -i re0 -n
```

## **Iperf**

While tools to measure network performance, such as ttcp, exist, most are very old and have confusing options. Iperf was developed as a modern alternative for measuring TCP and UDP bandwidth performance.

Iperf is a tool to measure maximum TCP bandwidth, allowing the tuning of various parameters and UDP characteristics. Iperf reports bandwidth, delay jitter, datagram loss.

<http://iperf.sourceforge.net/>

Postoji kao [PfSense paket](#).

## Za BSD

```
portmaster -n benchmarks/iperf
```

## Za GNU/Linux

```
emerge -a iperf
```

## **Unhide**

Is a forensic tool to find hidden processes and TCP/UDP ports by rootkits / LKMs or by another hidden technique. It consists of two programs: unhide and unhide-tcp.

<http://www.unhide-forensics.info/>

## Za BSD

```
portmaster -n security/unhide
```

Izvršne fajle su

```
unhide
```

```
unhide-tcp
```

<http://www.cyberciti.biz/tips/linux-unix-windows-find-hidden-processes-tcp-udp-ports.html>

## **SplitVT**

A program for splitting terminals into two shells

<http://slouken.libsdl.org/projects/splitvt>

## Za BSD

```
portmaster -n misc/splitvt
```

## Za GNU/Linux

```
emerge -a splitvt
```

## **Ettercap**

A suite for man in the middle attacks and network mapping

<http://ettercap.sourceforge.net>

Za [BSD](#)

```
portmaster -n net-mgmt/ettercap
```

Za [GNU/Linux](#)

```
emerge -a ettercap
```

```
ettercap --help
```

Ako hoćete [Ncurses](#)

```
ettercap -C
```

Ako hoćete GTK

```
ettercap -G
```

## **Wireshark**

A network protocol analyzer formerly known as ethereal

<http://www.wireshark.org>

Za [BSD](#)

Postoji [PBI](#) paket.

```
portmaster -n net/wireshark
```

## Za GNU/Linux

emerge -a wireshark

<https://wiki.archlinux.org/index.php/Wireshark>

Ako hoćete da koristite Wireshark kao normalni korisnik što on preporučuje, stavite se u njegovu grupu.

gpasswd -a normalni-korisnik wireshark

## **IPAudit**

Monitors network activity on a network by host, protocol and port

<http://ipaudit.sourceforge.net/>

## Za BSD

portmaster -n net-mgmt/ipaudit

## Za GNU/Linux

emerge -a ipaudit

ipaudit --help

ipstrings --help

## **Snort**

Libpcap-based packet sniffer/logger/lightweight IDS

<http://www.snort.org>

## Za BSD

```
portmaster -n security/snort
```

Za [GNU/Linux](#)

```
emerge -a snort
```

[BSD Magazine](#) je u sledećim izdanjima opisao [Snort](#)

03.2009

## **Snortsam**

[Snort](#) plugin that allows automated blocking of IP addresses on several firewalls

<http://www.snortsam.net>

Za [BSD](#)

```
portmaster -n security/snortsam
```

Za [GNU/Linux](#)

```
emerge -a snortsam
```

## **John the Ripper**

Fast Password cracker

<http://www.openwall.com/john/>

Za [BSD](#)

Postoji [PBI](#) paket.

```
portmaster -n security/john
```

Za [GNU/Linux](#)

```
emerge -a johntheripper
```

Koristi ga [WepAttack](#).

Možete probati da proverite svoje šifre, to jest da li su [dovoljno jake](#).

```
unshadow --help
```

Napravite privremenu fajlu sa Vašim šiframa na primer sa

```
unshadow /etc/passwd /etc/shadow > ~/šifre.txt
```

Zaštite tu fajlu

```
chown root:root ~/šifre.txt
```

```
chmod 600 ~/šifre.txt
```

Startajte [John the Ripper](#) da proverite Vaše šifre

```
john ~/šifre.txt
```

Svaki put kad pritisnete enter javiće Vam šta je uradio

```
guesses: 0 time: 0:00:01:18 4.80% (2) (ETA: vreme) c/s: 320 trying: Montrose - Perfect
```

Možete videti da li je našao sa

```
john -show ~/šifre.txt
```

```
0 password hashes cracked, 4 left
```

Kad ste završili sa ispitivanjem Vaših šifri izbrišite tu fajlu sa

```
rm -f ~/šifre.txt
```

## Ophcrack

A time-memory-trade-off-cracker and tables

<http://ophcrack.sourceforge.net>

Za [BSD](#)

```
portmaster -n security/ophcrack
```

Za [GNU/Linux](#)

```
emerge -a ophcrack ophcrack-tables
```

## Packit

Network auditing tool that allows you to monitor, manipulate, and inject customized IPv4 traffic

<http://www.packetfactory.net/projects/packit/>

Za [BSD](#)

```
portmaster -n net-mgmt/packit
```

Za [GNU/Linux](#)

```
emerge -a packit
```

## tail

Za [BSD](#)

[tail](#) se nalazi u [FreeBSD Base paketima](#).

Za [GNU/Linux](#)

[tail](#) se nalazi u paketu [Coreutils](#).

```
tail --help
```

```
info coreutils 'tail invocation'
```

```
tail -f -n 10 /var/log/messages
```

```
tail -f -n 10 /var/log/messages | grep ssh
```

## **turbotail**

drop-in replacement for [tail](#) which uses the [GNU/Linux Kernel](#) DNOTIFY-api

<http://www.vanheusden.com/turbotail/>

Za [GNU/Linux](#)

```
emerge -a turbotail
```

## **MultiTail**

Tail with multiple windows.

<http://www.vanheusden.com/multitail/index.html>

Za [BSD](#)

```
portmaster -n sysutils/multitail
```

Za [GNU/Linux](#)

```
emerge -a multitail
```

```
multitail --help
```

## **root-tail**

Terminal to display (multiple) log files on the root window

Terminal koji prikazuje log fajle u root prozoru.

<http://www.goof.com/pcg/marc/root-tail.html>

Za [BSD](#)

```
portmaster -n sysutils/roottail
```

Za [GNU/Linux](#)

```
emerge -a root-tail
```

```
root-tail --help
```

Malo uputstvo kako da ispitujete Wireless

<http://www.bsd-srbija.org/viewtopic.php?id=699>

## Aircrack-ng

WLAN tools for breaking 802.11 WEP/WPA keys

Za ispitivanje WLAN 802.11 WEP/WPA ključeva

<http://www.aircrack-ng.org/>

Za [BSD](#)

```
portmaster -n net-mgmt/aircrack-ng
```

Za [GNU/Linux](#)

```
emerge -a aircrack-ng
```

## WepAttack

Is a WLAN [Open Source GNU/Linux](#) tool for breaking 802.11 WEP keys. This tool is based on

an active dictionary attack that tests millions of words to find the right key.

Može da koristi [John the Ripper](#).

<http://wepattack.sourceforge.net/>

```
emerge -a wepattack
```

## ARP Counterattack

Is a program for detecting and remedying "ARP attacks." It monitors traffic on any number of Ethernet interfaces and examines ARP replies and gratuitous ARP requests. If it notices an ARP reply or gratuitous ARP request that is in conflict with its notion of "correct" Ethernet/IP address pairs, it logs the attack if logging is enabled, and, if the Ethernet interface that the attack was seen on is configured as being in aggressive mode, it sends out a gratuitous ARP request and a gratuitous ARP reply with the "correct" Ethernet/IP address pair in an attempt to reset the ARP tables of hosts on the local network segment. The corrective gratuitous ARP request and corrective gratuitous ARP reply can be sent from an Ethernet interface other than the one that the attack was seen on.

[http://acm.poly.edu/wiki/ARP\\_Counterattack](http://acm.poly.edu/wiki/ARP_Counterattack)

Za [BSD](#)

```
portmaster -n security/arpCounterattack
```

## Kismet

IEEE 802.11 wireless LAN sniffer

Za ispitivanje IEEE 802.11 wireless LAN sniffer

<http://www.kismetwireless.net/>

Za [BSD](#)

```
portmaster -n net-mgmt/kismet
```

Za [GNU/Linux](#)

```
emerge -a kismet
```

## **Metasploit**

Advanced open-source framework for developing, testing, and using vulnerability exploit code

<http://www.metasploit.org>

Za [BSD](#)

```
portmaster -n security/metasploit
```

Za [GNU/Linux](#)

```
emerge -a net-analyzer/metasploit
```

## **THC-Hydra**

Is a parallelized login hacker utility. Hydra can brute force attack on FTP, POP3, IMAP, [Telnet](#), HTTP Auth, NNTP, VNC, ICQ, Socks5, PCNFS and more services within SSL support. This port is provided as a standalone program to avoid installing a full Nessus scanner system.

<http://www.thc.org/thc-hydra/>  
<http://freeworld.thc.org/thc-hydra/>

Za [BSD](#)

```
portmaster -n security/hydra
```

Za [GNU/Linux](#)

```
emerge -a net-analyzer/hydra
```

```
man hydra
```

```
man pw-inspector
```

```
man xhydra
```

## **DoS Detector**

Tool to analyze and detect suspicious traffic from IP and alert about it

Ne instalijete DoS Detector, jer on kad se starta restartuje kompjuter, bar kod mene.

<http://darkzone.ma.cx/resources/unix/dosdetector/>

Za [BSD](#)

```
portmaster -n net/dosdetector
```

Za [GNU/Linux](#)

```
emerge -a net-analyzer/dosdetector
```

## Rootkit Hunter

Scans for known and unknown rootkits, backdoors, and sniffers

<http://rkhunter.sf.net/>

Za [BSD](#)

Postoji [PBI](#) paket.

```
portmaster -n security/rkhunter
```

Za [GNU/Linux](#)

```
emerge -a rkhunter
```

```
rkhunter --help
```

Za [BSD](#)

Možete staviti u

/etc/periodic.conf

```
# You should keep your rkhunter database up-to-date.  
# This can be done automatically by putting this line to /etc/periodic.conf:
```

```
daily_rkhunter_update_enable="YES"
daily_rkhunter_update_flags="--update --nocolors"

# Also, you can run rkhunter as a part of the daily security check by
# putting this line to /etc/periodic.conf:

daily_rkhunter_check_enable="YES"
daily_rkhunter_check_flags="--checkall --nocolors --skip-keypress"
```

Proverava ceo sistem na instalirane root-kitt-ove, potrebno ako imate neki Server

```
rkhunter -c --sk
```

Da obnovite database

```
rkhunter --propupd
```

## **Chkrootkit**

A tool to locally check for signs of a rootkit

Koristite [Chkrootkit](#) zajedno sa [Rootkit Hunter](#)-om, tako možete povećati sigurnost

<http://www.chkrootkit.org>

Za [BSD](#)

```
portmaster -n security/chkrootkit
```

Za [GNU/Linux](#)

```
emerge -a chkrootkit
```

```
chkrootkit --help
```

Izvršite samo

chkrootkit

Podesite da se izvršava nedeljno u /etc/cron.weekly

## Tripwire

[Free Software](#) File Integrity Checker and IDS

<http://www.tripwire.org/>

<http://sourceforge.net/projects/tripwire/>

Za [BSD](#)

portmaster -n security/tripwire-verzija

Za [GNU/Linux](#)

emerge -a tripwire

## AIDE, Advanced Intrusion Detection Environment

Is a replacement for [Tripwire](#)

<http://aide.sourceforge.net/>

Za [BSD](#)

portmaster -n security/aide

Za [GNU/Linux](#)

emerge -a aide

aide --help

man aide

Treba da inicijalizujete [AIDE](#)

```
cd /var/db/aide  
aide --init  
mv databases/aide.db.new databases/aide.db
```

## Kako se koriste ovi programi

### Portovi

GTK [GUI](#) za [Nmap](#), veoma dobar

Kao normalni korisnik

```
zenmap
```

Normalno samo [root](#) treba da koristi [Nmap](#) i [Zenmap](#)

Da se lako ulogujete kao [root](#)

```
uxterm -e su -m root -c zenmap %F
```

Ovo je predlog od instalacije, koristi se [Bash](#) skripta koja u [FreeBSD](#) ne radi

```
/usr/share/zenmap/su-to-zenmap.sh %F
```

Da bi znali kako se tačno [Nmap](#) koristi

```
nmap --help
```

Možete pingovati kao [root](#) i one mašine u lokalnoj mreži koje ne dopuštaju ICMP echo request

```
nmap -T5 -sP 192.168.1.0/24
```

Provera portova

```
nmap -p 1-1024 IP-adresa
```

Provera svega

```
nmap -O IP-Adresa
```

Provera opsega adresa

```
nmap -sS 10.0.1.0-30
```

Nalazi skoro sve

```
nmap -v -A IP-adresa
```

Da vidite malo više

```
nmap -vvv -A IP-adresa
```

Veći opseg adresa

```
nmap -v -sn 192.168.0.0/16
```

```
nmap -v -sn 10.0.0.0/8
```

Sve Portove, traje veoma dugo

```
nmap -v -A -p 1-65535 IP-adresa
```

```
nmap -sA -p 1-65535 IP-adresa
```

Da vidite koji su Vam Port-ovi otvoreni lokalno

```
nmap -sV localhost -p 1-65535
```

Provera portova

```
hping --scan 1-1024 -S IP-Adresa
```

Da vidite koji program koristi taj Port

```
lsof -i :Port
```

```
lsof | grep broj-Port-a
```

## Konekcije

Pogledajte [net-tools](#) i [iproute2](#)

```
netstat --help
```

Koji portovi su otvoreni

```
netstat -an | grep LISTEN
```

```
netstat -tunap
```

Koji portovi su otvoreni (samo server)

```
netstat -tulpn | more
```

```
netstat -tulpn | less
```

Aktivne internet konekcije (samo serveri)

```
netstat -lp
```

Aktivne internet konekcije (bez servera)

```
netstat -tu
```

Koliko konekcija postoji, numerički samo, skraćeno

```
netstat -an | awk '/^tcp/ {A[$(NF)]++} END {for (l in A) {printf "%5d %s\n", A[l], l}}'
```

Koliko ima konekcija i objašnjenja

```
netstat -s -t
```

Koji programi koriste 127.0.0.1 ili localhost

```
lsof -i -n -P | grep -v 127.0.0.1
```

Koje konekcije postoje

```
cat /proc/net/ip_conntrack | less
```

Kernel IP routing table

```
netstat -rn
```

Broj konekcija

```
netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr | more
```

Neprekidno aktivne konekcije sa i bez servera

```
/home/bin/netstat-split
```

## Hosts

DiG lista opcija, dig je iz [GNU/Linux Kernel](#)-a

```
dig -h
```

Pokazuje koja adresa IP Provajdera Vašoj dinamičkoj adresi

```
dig Vaša-dinamička-adresa
```

Da pronađete dinamičku adresu

```
dig -x IP-adresa-od-Provajdera
```

Nalaženja IP adresa

```
host -a www.adresa
```

```
nslookup www.adresa
```

```
nslookup adresa
```

Obrnuta kontrola od te www.adrese ili adrese

```
host -a IP- adresa
```

```
whois IP-adresa
```

```
nslookup IP-adresa
```

Da vidite u kojoj zemlji je koja stranica, bez ili sa www

```
geoiplookup www.adresa
```

Malo informacija o stranicama

<http://www.sitedossier.com/>

<http://www.sitedossier.com/site/ns-linux.org>

Nalaženje mesta, ako imate IP adresu

<http://www.ipaddresslocation.org/ip-address-locator.php>

<http://software77.net/geo-ip/>

## MAC adrese

Da menjate MAC adresu možete koristiti [GNU MAC Changer](#)

Prikaz Vaše MAC adresu u default [GNU/Linux](#) stilu

```
arp -e
```

Pokazuje Vaše MAC adresu u [BSD](#) stilu

```
arp -a
```

Lista opcija sa ovom komandom

```
packit
```

Prikazuje šta se sve dešava na eth0

```
tcpdump -i eth0 -e -X -vv
```

Prikazuje šta se sve dešava na određenoj IP adresi

```
tcpdump -i eth0 host IP-adresa
```

## Obavezno obnavljajte sistem

i pakete sa

### Za BSD

```
portsnap fetch update
```

```
portmaster -a -y -D
```

### Za Portage

```
emerge --sync && layman -S && eix-update
```

```
emerge -auvND world
```

### Za Paludis

```
cave sync
```

```
cave resolve world --complete
```

**Jer samo tako možete ispraviti greške programa, pogrešne verzije, koji mogu da cure informacije.**

### Kontrola

Posetite obavezno ove i ostale stranice koje pišu o sigurnosti

Ne koristite za pretraživanje Interneta Google

Redovno pregledajte sistemske log fajle

Koji programi postoje za kontrolu

Kako se koriste ovi programi

Portovi

Konekcije

Hosts

MAC adrese

[Obavezno obnavljajte sistem](#)  
[Na početak](#)

## **Kontrola u X-u**

**Ovo je esencijalna stvar, treba da se zna šta se dešava ispod haube, jer to povećava sigurnost i upotrebljivost [GNU/Linux-a](#).**

**Mnogi zaborave jednostavno da prate šta se sa resursima dešava i retko koriste [programe za Kontrolu](#). Dok negde ne zaškripi. Mada često ni tada nisu svesni.**

**Sve je u redu dok neki program ne javi neku grešku da ili imaju premalo memorije ili  
je CPU često suviše zauzet i nema pomisli na neki ozbiljniji rad.**

**Navika ne postoji da se gleda šta se dešava u [/var/log](#).**

[Proverite da li je neki program zaostao ako ste restartovali X.](#)

To sve i više možete imati stalno pred očima u X-u sa sledećim programima, najviše koristim [top](#), [Atop](#), [htop](#), [Conky](#) i [Etherape](#).

**Pogledajte i [programe koji prikazuju razne Hardware informacije](#).**

### **Conky**

An advanced, highly configurable system monitor for X

<http://conky.sourceforge.net>

Za [BSD](#)

Postoji [PBI](#) paket.

portmaster -n sysutils/conky

Za [GNU/Linux](#)

emerge -a conky

Za one koji vole da znaju šta se radi ispod haube i ne vole da imaju samo osnovne stvari, ovo je veoma dobar program.

On se mora podešavati ručno, da bi mogao ispunjavao skoro sve Vaše potrebe za Monitoring-om i drugim stvarima. On se veoma lako dopunjava.

<http://www.linux.com/feature/136147>

[http://wiki.fluxbox.org/index.php?title=Conky\\_Panel\\_Type](http://wiki.fluxbox.org/index.php?title=Conky_Panel_Type)

<http://ubuntuforums.org/showthread.php?t=281865>

<http://conky.linux-hardcore.com/>

<http://www.sakharin.com/node/6>

Kanal #conky na [Freenode](#)

On se upravlja preko

~/.conkyrc

Morate paziti, on je veoma osetljiv na sintaksu, kao svaki program, ako samo jedan znak nedostaje, a treba tu da bude, on ne starta Vašu konfiguraciju.

Imajte zato uvek osiguranja.

```
cp -a ~/.conkyrc ~/.conkyrc-00
```

Postoji i mogućnost da se koriste više sesija [Conky-a](#), sa potpuno različitim opcijama.

Gornji deo im je isti, jedina razlika je u

položaju prozora

veličini prozora

imenu konfiguracije

Ispod "TEXT" varijable su specifične opcije za svaku konfiguraciju.

Nazovite ih različito kao na primer

~/.conkyrc-Hardware

~/.conkyrc-Internet

~/.conkyrc-HDD

~/.conkyrc-System

Onda ih zovete sa

```
conky -c .conkyrc-neka
```

Mada je mnogo bolji način da u svakoj fajli dopišete na prvom mestu

```
#!/usr/bin/conky -c
```

Napravite da su fajle izvršne

```
chmod u+rx ./conkyrc-neka
```

Čim pritisnete na tu fajlu ili je tako pozovete iz [Fluxbox menija](#), odmah se starta Conky sa tom konfiguracijom.

```
...
[exec] (Conky Hardware) {~/.conkyrc-Hardware} <>
[exec] (Conky Internet) {~/.conkyrc-Internet} <>
[exec] (Conky HDD) {~/.conkyrc-HDD} <>
[exec] (Conky System) {~/.conkyrc-System} <>
...
```

A još uvek imate i mogućnost da koristite default .conkyrc za probe.

Ja na primer koristim:

Hardware Monitoring

.conkyrc-Hardware

Kako se [Internet](#) koristi. Koje konekcije su ostvarene, koji Port-ovi se koriste. Netstat.

.conkyrc-Internet

Pregled Harddisk-ova, koliko su vrući, koliko i kako se koriste, koliko su particije zauzete.

.conkyrc-HDD

Posmatranje najvažnijih poruka iz /var/log

/var/log/messages  
/var/log/syslog-ng/sshd.log  
/var/log/syslog-ng/kernel.log

...

.conkyrc-System

Da bi te poruke mogao korisnik da gleda

/home/bin/chown-messages

Da bi razne konfiguracije dobro radile morate na primer u .conkyrc-Hardware imati

...

# Title Manually set the window name. Defaults to "<hostname> - conky"  
own\_window\_title Conky Hardware

...

Na Internetu imate toliko primera da Vam uopšte nije teško napraviti konfiguracije koje Vama odgovaraju.

Moje probe su u /paketi/Hardware/Hardware Monitor/Conky/posebni-direktorijumi

Kad isprobavam razne konfiguracije sa Interneta, mnogo mi pomaže ova fajla

/home/bin/touch-c

Da bi imali kontrolu nad puno verzija svake konfiguracije

Uđite u Vaš matični direktorijum

cd

Napravite direktorijum

```
mkdir ./conky
```

Prebacite Vaše konfigracije

```
mv ./conkyrc* ./conky/
```

Linkujte ove fajle da bih Conky našao

```
ln -s ./conky/.conkyrc-Hardware ./conkyrc-Hardware
```

```
ln -s ./conky/.conkyrc-Internet ./conkyrc-Internet
```

```
ln -s ./conky/.conkyrc-HDD ./conkyrc-HDD
```

```
ln -s ./conky/.conkyrc-System ./conkyrc-System
```

A u tom direktorijumu možete imati šta god poželite a da nemate nered u  
~/ Vašem matičnom direktorijumu.

Takođe preporučujem da napravite jedan direktorijum za osiguranja

```
mkdir ~/conky-save
```

Osigurajte ponekad sa, počnite od 00

```
cp -a ./conky ./conky-save/conky-neki-dvocifreni-broj
```

Boje koje možete koristiti su definisane u

```
cat /usr/share/X11/rgb.txt | more
```

[Ako hoćete da sa Conky vidite vreme u X-u](#)

*Kraj Conky*

## **GKrellM**

With a single process, [GKrellM](#) manages multiple stacked monitors and supports applying themes to match the monitors appearance to your window manager, Gtk, or any other theme.

Za one koje vole jednostavno, ovo je "pravi" program, ima samo dosta stvari.

<http://www.gkrellm.net>

Da vidite šta ima

Za [BSD](#)

```
find /usr/ports/* | grep gkrellm
```

Za [GNU/Linux](#)

```
eix gkrellm
```

Za [BSD](#)

Postoji [PBI](#) paket.

```
portmaster -n sysutils/gkrellm2
```

Za [GNU/Linux](#)

```
emerge -a gkrellm ....
```

## **System Monitor**

Process viewer and system resource monitor for [Gnome](#)

<http://library.gnome.org/users/gnome-system-monitor/>

```
emerge -a gnome-system-monitor
```

## **QtSystemInfo**

Is a useful class that provides information on the currently running system (like system type, name and version, [GNU/Linux Kernel](#) Name and version).

Nije baš ništa bolja od komande uname -a.

<http://qt-apps.org/content/show.php/QtSystemInfo?content=122436>

[Instališe se ručno](#) i to na način za [Qt programe](#).

## **KSysguard**

A network enabled task manager and system monitor application

[KDE](#) program

Za one koji hoće jednostavno, nema puno opcija, koristio sam ga pre puno, a sad nikako.

```
emerge -a ksysguard
```

## **Nagios**

<http://www.nagios.org>

```
eix nagios
```

Pa šta Vam treba, nisam ga probao.

Ovo je samo osnova i šta još hoćete

```
emerge -a nagios-core ...
```

Ako hoćete sve ovo je meta paket

```
emerge -a nagios
```

[Kontrola u X-u](#)  
[Conky](#)  
[Gkrellm](#)  
[KSysguard](#)  
[Nagios](#)  
[Na početak](#)

## **SSH protokol**

Da vidite šta ima za [BSD](#)

```
cd /usr/ports/security/ ; ls | grep ssh
```

**Nije preporučljivo koristiti ssh kao [Administrator \(root\)](#). Mada se nekad i to mora u nekim velikim mrežama, nemate tu nekog velikog izbora.**

**Ako koristite [root](#) za [OpenSSH](#) samo za [Rsync](#) ili [Distcc](#), ali samo sa [OpenSSH ključevima](#), onda je to izuzetak koji potvrđuje pravilo.**

**Koristite gde to možete [SSH Tunnel-e](#), veoma povećava sigurnost.**

**SSH koristite kao [korisnika za logovanja](#), koji nema puno prava, sem da je u wheel grupi pa možete koristiti su komandu da se ulogujete kao [root](#). Koristite ako možete samo u lokalnu [normalnog korisnika](#).**

**To povećava sigurnost jer niko se ne može ulogovati kao [root](#) i mora da zna prvo koji Port se koristi, koji korisnik, korisničku šifru tog [korisnika za logovanja \(15 znakova\)](#), šifru [Administrator \(root\)-a \(15 znakova\)](#) i eventualno od [Vašeg ključa za OpenSSH \(15 znakova, Keychain to traži\)](#).**

**Što veoma povećava sigurnost, da neko nepoželjan preko ssh-a može da uđe u sistem. Skoro je nemoguće da se to desi.**

Možete smanjiti prava samo scp da je dopušten

[http://freebsdrocks.net/index.php?option=com\\_content&view=article&id=108:chroot-scp-users-using-ssh&catid=20:customizing-your-freebsd-box&Itemid=25](http://freebsdrocks.net/index.php?option=com_content&view=article&id=108:chroot-scp-users-using-ssh&catid=20:customizing-your-freebsd-box&Itemid=25)

**Sve ovo treba obavezno pročitati**

<http://www.gentoo.org/doc/en/articles/openssh-key-management-p1.xml> p2, p3

<https://wiki.archlinux.org/index.php/SSH>

<http://fedorasolved.org/post-install-solutions/securing-ssh>

<http://www.linux.com/articles/61061>

Nemački odlično, puno tema je dobro obrađeno, vredi prevesti

<http://www.jfranken.de/homepages/johannes/vortraege/ssh1.de.html>

Staro ali odlično

<http://www.employees.org/~satch/ssh/faq/ssh-faq.html>

Kako da analizirate pogrešne pokušaje SSH logovanja

<http://www.securityfocus.com/infocus/1876>

<http://www.symantec.com/connect/articles/analyzing-malicious-ssh-login-attempts>

## OpenSSH

Port of [OpenBSD](#)'s free SSH release

Je osnova za SSH protokol, može se koristiti i za [Router](#).

<http://www.openssh.org/>

<http://www.openssh.com/faq.html>

[http://www.openbsd.org/cgi-bin/man.cgi?query=sshd\\_config](http://www.openbsd.org/cgi-bin/man.cgi?query=sshd_config)

[http://www.openbsd.org/cgi-bin/man.cgi?query=ssh\\_config](http://www.openbsd.org/cgi-bin/man.cgi?query=ssh_config)

<http://www.freebsd.org/doc/handbook/openssh.html>

[https://en.wikipedia.org/wiki/Secure\\_Shell](https://en.wikipedia.org/wiki/Secure_Shell)

Ako hoćete da [OpenSSH](#) i scp rade brže pogledajte

<http://www.psc.edu/networking/projects/hpn-ssh/>

<http://www.psc.edu/networking/projects/tcptune/>

Za [BSD](#)

[OpenSSH](#) se nalazi u [FreeBSD Base paketima](#).

Ako hoćete da koristite u [BSD](#)-u noviji [OpenSSH](#)

portmaster -n crypto/openssh

Da se uvek starta pri podizanju sistema

[/etc/rc.conf](#)

```
sshd_enable="YES"
```

Za [GNU/Linux](#)

Dodajte USE hpn

```
net-misc/openssh -ldap X509 hpn
```

```
emerge -a openssh
```

Omogućite da se [SSH](#) Deamon podigne pri svakom startanju sistema

```
rc-update add sshd default
```

```
man sshd
```

```
man ssh_config
```

Pogledajte i [Upotreba OpenSSH-a.](#)

## **Dodatni programi za [SSH protokol](#)**

### **Keychain**

Manage [SSH](#) and [GnuPG](#) keys in a convenient and secure manner.  
Frontend for ssh-agent/ssh-add

Omogućava da se automatski sa [SSH](#) ulogujete bez šifre, ako ste se već jedanput uspešno ulogovali. Takođe i da koristite za razne svrhe [GnuPG](#) ključeve a da ih novo ne pišete.

<http://www.funtoo.org/en/security/keychain/intro/>

<http://www.gentoo.org/doc/en/keychain-guide.xml>

Za [BSD](#)

```
portmaster -n security/keychain
```

Za [GNU/Linux](#)

```
emerge -a keychain
```

Da prekinete [Keychain](#) da se novo učitaju ključevi i podešavanja, ako nešto nije u redu

```
keychain --clear
```

```
keychain -k
```

Stavite u Vašu [Shell](#) fajlu, da se uvek učita i da ne smetaju poruke na primer za [GKSu](#)

Za [tcsh](#)

```
~/.cshrc
```

```
# Start Keychain at login
# on this next line, we start keychain and point it to the private keys that
# we'd like it to cache
keychain ~/.ssh/id_dsa >&! /dev/null
source ~/.keychain/$HOST-csh-gpg >&! /dev/null
```

Za [Bash](#)

```
~/.bash_profile
```

```
# Start Keychain at login
# example ~/.bash_profile file
# on this next line, we start keychain and point it to the private keys that
# we'd like it to cache
/usr/bin/keychain ~/.ssh/id_dsa > /dev/null 2>&1
```

[Možete menjati šifru za OpenSSH ključeve](#)

## Autossh

Is a program to start a copy of [SSH](#) and monitor it, restarting it as necessary should it die or stop passing traffic.

The original idea and the mechanism were from [rstunnel](#) (Reliable SSH Tunnel). With this version the method changes: autossh uses ssh to construct a loop of ssh forwardings (one from local to remote, one from remote to local), and then sends test data that it expects to get back. (The idea is thanks to Terrence Martin.)

Može se koristiti i za [Router](#).

<http://www.harding.motd.ca/autossh/>

<http://www.gentoo-wiki.info/Autossh>

Za [BSD](#)

Postoji [PBI](#) paket, posle mog predloga od 01.04.2012.

```
portmaster -n security/autossh
```

Za [GNU/Linux](#)

```
emerge -a autossh
```

```
autossh --help
```

```
man autossh
```

Da bi to radilo morate propustiti 2 dodatna viša TCP Port-a, što je manje sigurno.

Sam Autor kaže na stranici i u manualu kao i [Gentoo](#) Wiki da ako koristite noviju Verziju [OpenSSH](#) i koristite sledeće opcije za njega

kod Servera ClientAliveInterval, ClientAliveCountMax

kod Klijenta ServerAliveInterval, ServerAliveCountMax

Onda trebate da isključite korišćenje Port-ova za autossh i onda ovako izgleda komanda

```
autossh -M 0 -p viši-Port korisnik-za-logovanja@neka-adresa
```

Umesto normalne komande

```
ssh -p viši-Port korisnik-za-logovanja@neka-adresa
```

Stavite na primer u

Za [tcsh](#)

```
/etc/csh.cshrc
```

```
# To use Autoshh without Port
alias ssh 'autoshh -M 0'

# To have normal OpenSSH with enabled Autoshh
alias ssh- ssh
```

Za [Bash](#)

```
/etc/bash/bashrc
```

```
# To use Autoshh without Port
alias ssh='autoshh -M 0'

# To have normal OpenSSH with enabled Autoshh
alias ssh='ssh'
```

## ScanSSH

Network scanner that gathers info on [SSH](#) protocols and versions

Skenira [SSH](#) protokol

<http://monkey.org/~provos/scanssh/>

Za [BSD](#)

```
portmaster -n security/scanssh
```

Za [GNU/Linux](#)

```
emerge -a scanssh
```

## **SecPanel**

Graphical frontend for managing and running [SSH](#) and SCP connections

Omogućava grafički da ostvarujete [SSH](#) konekcije, nije potrebno to je samo šminka

<http://themediahost.de/secpanel/>

Za [BSD](#)

```
portmaster -n security/secpanel
```

Za [GNU/Linux](#)

```
emerge -a secpanel
```

## **Putty**

UNIX port of the famous [Telnet](#) and [SSH](#) client

Koristim ga većinom samo za serijski protokol. [Za flašovanje rutera je odličan.](#)

Za [Telnet](#) pristup možete koristiti i [Netcat](#).

Može se koristiti i za [smopu!M](#).

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

[http://www.jfitz.com/tips/ssh\\_for\\_windows.html](http://www.jfitz.com/tips/ssh_for_windows.html)

[http://www.jfitz.com/tips/putty\\_config.html](http://www.jfitz.com/tips/putty_config.html)

Za [BSD](#)

Postoji [PBI](#) paket.

```
portmaster -n security/putty
```

Za [GNU/Linux](#)

```
emerge -a putty
```

Da imate bolje fontove za [Putty](#). Odličan je font terminal (bitstream).

<http://malektips.com/putty-font-anti-aliasing.html>

## **rssh**

Is a Restricted Secure SHell that allow only the use of sftp or scp. It could be used when you need an account (and a validshell) in order to execute sftp or scp but when you don't want to give the possibility to log in to this user.

<http://www.pizzashack.org/rssh/>

Za [BSD](#)

```
portmaster -n shells/rssh
```

Za [GNU/Linux](#)

```
emerge -a rssh
```

## **scponly**

Is an alternative "shell" (of sorts) for system administrators who would like to provide access to remote users to both read and write local files without providing any remote execution privileges. Functionally, it is best described as a wrapper to the tried-and-true [SSH](#) suite.

<http://sublimation.org/scponly/wiki/>

Za [BSD](#)

```
portmaster -n shells/scponly
```

Za [GNU/Linux](#)

```
emerge -a scponly
```

[SSH Protokol](#)

[OpenSSH](#)

[Dodatni programi za SSH protokol](#)

[Keychain](#)

[Autossh](#)  
[ScanSSH](#)  
[SecPanel](#)  
[Putty](#)  
[rssh](#)  
[scponly](#)  
[Ključevi za OpenSSH](#)  
[Primer podešavanja za OpenSSH](#)  
[Možete koristiti root nalog za OpenSSH](#)  
[SSH Tunnel](#)  
[Upotreba OpenSSH-a](#)  
[Na početak](#)

## **Ključevi za [OpenSSH](#)**

Koristite samo DSA ključeve i Protocol 2. To je jednostavno sigurnije.

While RSA keys are used by version 1 of the ssh protocol, DSA keys are used for protocol level 2, an updated version of the ssh protocol. Any modern version of [OpenSSH](#) should be able to use both RSA and DSA keys. Generating DSA keys using [OpenSSH](#)'s ssh-keygen can be done similarly to RSA in the following manner:

Nowadays you should only use version 2 of the ssh protocol, as version 1 has weaknesses.

**Dakle i dalje se traži šifra za Vaš ključ, ali ne za logovanje.**

**[Šifre moraju biti veoma jake.](#)**

**Mogu se ovi ključevi koristiti i za [SSHFS, SSH Filesystem](#). Radi odlično.**

**Ako se ključ napravi bez šifre onda se može ulogovati i bez šifre na poznate lokacije ako se razmene ključevi. Oprezno koristite samo u lokalnu na Vašim kompjuterima.**

**Koristiti sa oprezom, ne preporučujem da koristite za Laptop-ove, jer se mogu izgubiti ili neko doći do Vašeg ključa.**

<http://www.ibm.com/developerworks/library/l-keyc.html>

<http://www.gentoo.org/doc/en/articles/openssh-key-management-p1.xml>

<http://lackof.org/taggart/hacking/ssh/>

<http://mywiki.woolege.org/SshKeys>

<http://www.howtoforge.com/set-up-ssh-with-public-key-authentication-debian-etch>

<http://www.ualberta.ca/CNS/RESEARCH/LinuxClusters/pka-openssh.html>

<http://www.bluegum.com/Software/ssh-auth.html>

[https://wiki.archlinux.org/index.php/Using\\_SSH\\_Keys](https://wiki.archlinux.org/index.php/Using_SSH_Keys)

<http://www.faqs.org/docs/securing/chap15sec121.html>

Naravno originalna dokumentacija je veoma važna

man ssh-keygen

man ssh-add

**Koristite jaku šifru kao za root-a, nju će Vam tražiti i Keychain**

Normalna je komanda

**ssh-keygen -t dsa**

Pazite navedite punu putanju i ime ključa, na primer

**/home/user/.ssh/id\_dsa**

**Poželjno je da su Vaši javni ključevi u obliku**

**ssh-dss ...== korisnik@hostname**

**Možete navesti i ime za taj ključ da bude na primer privat\_dsa ili server-a\_dsa, server-b\_dsa, ako imate više različitih mreža.**

**ssh-keygen -t dsa -f ~/.ssh/privat\_dsa**

Za menjanje šifre za OpenSSH, posle mesec dva

ssh-keygen -p -f ~/.ssh/id\_dsa

ssh-keygen -p -f ~/.ssh/privat\_dsa

ssh-keygen -p -f ~/.ssh/games\_dsa

Ako ste izgubili Vaš id\_dsa.pub, možete ga ponovo napraviti od Vašeg privatnog ključa

```
ssh-keygen -y -f ~/.ssh/id_dsa
```

Fingerprint da proverite

```
ssh-add -l id_dsa.pub
```

Napravite ove fajle

```
touch ~/.ssh-agent
```

```
~/.bashrc
```

Za [Keychain](#), da se može automatski ulogovati bez šifre

```
touch ~/.bash_profile
```

```
~/.bash_profile
```

Bolje je u [konzoli](#) posle uspešnog logovanja da se navede pravilno keychain šifra.  
U [X](#)-u može da bude teže.

## Više ključeva za različite mreže

Ako imate više vrsta korisnika one kojima verujete i one kojima ne verujete,  
možete za one kojima bezuslovno verujete da napravite bez šifre.

**Pazite dobro kome dajete te ključeve bez šifre, budite veoma oprezni!**

Obavezno imajte i jedan ključ sa šifrom za ostale korisnike.

Trebate imati na primer

```
~/.ssh/privat_dsa  
~/.ssh/server-a_dsa  
~/.ssh/server-b_dsa
```

Onda se mora kad se hoće konektovati na taj server upotrebiti

```
ssh -i ~/.ssh/server-a_dsa -p xxxx korisnik-za-logovanja@server
```

Bolje je da podesite [Lična podešavanja za OpenSSH](#)

## Prenošenje SSH ključeva

### SSH-installkeys

Omogućava da prenesete ključ na drugu stranu, manuelno je bolje.

<http://www.catb.org/~esr/ssh-installkeys>

```
emerge -a ssh-installkeys
```

Gde hoćete da instalijete ključeve

```
ssh-installkeys -p xxxx korisnik-za-logovanja@192.168.1.4
```

Ovaj program dobro radi ali samo ako treba da bude samo sa Vaše strane jedan javni ključ na datom Serveru. Inače nekad prebriše postojeći javni a nekad ne kopira vaš javni ključ.

## Podprogram od [OpenSSH](#)-a

Prenosi public ključeve, nisam probao

```
/usr/bin/ssh-copy-id
```

Kao prividni korisnik

```
ssh-copy-id -i id_dsa.pub korisnik-za-logovanja@host
```

## Manuelan način prenošenja SSH ključeva

Koji sve isto radi ali tačno znate šta ste uradili. Preporučujem.

Može i duga komanda koja sve to odjednom radi, znači kopira ključ, proverava na obe strane prava, pravi fajlu authorized.keys, ako ne postoji. Ali može dodati isti ključ ako već postoji, proveriti i eventualni duplikat izbrisati. Možete koristiti ovu skriptu

```
/home/bin/ssh-installkeys-
```

Prvo morate manuelno preneti Vaš javni ključ na drugu stranu

```
scp -P xxxx ~/.ssh/id_dsa.pub korisnik-za-logovanja@192.168.1.4:~/  
ssh -p xxxx korisnik-za-logovanja@192.168.1.4
```

To sprečava da Vaš ključ prebriše neki drugi javni koji već postoji, ako fajla `~/.ssh/authorized_keys` ne postoji ovom komandom će se napraviti

```
cat ~/id_dsa.pub >> ~/.ssh/authorized_keys
```

```
rm -f ~/id_dsa.pub
```

Ili

```
cat /podaci/privat_dsa.pub >> ~/.ssh/authorized_keys  
rm -f /podaci/privat_dsa.pub
```

Ako ste na neki drugi način preneli Vaš javni ključ i nalazi se u

```
/podaci/Razmena/hostname-ssh.tar.bz2
```

```
cd /podaci/Razmena  
mkdir hostname-ssh  
tar xfj hostname-ssh.tar.bz2 -C ./hostname-ssh  
cd hostname-ssh
```

Uđite gde trebate

```
cd gde-je-Vaš-ključ  
cat Vaš-dsa.pub >> ~/.ssh/authorized_keys
```

ili

```
cat Vaš-dsa.pub >> /home/Vaš-user/.ssh/authorized_keys
```

Obrišite taj privremeni direktorijum i ako hoćete paket sa

```
cd /podaci/Razmena  
rm -rf hostname-ssh*
```

Dajte sigurne dozvole, da Vaš direktorijum i fajle budu sigurne

```
chmod 700 ~/.ssh  
chmod 600 ~/.ssh/*
```

[SSH Protokol](#)  
[OpenSSH](#)  
[Dodatni programi za SSH protokol](#)  
[Ključevi za OpenSSH](#)  
[Više ključeva za različite mreže](#)  
[Prenošenje SSH ključeva](#)  
[SSH-installkeys](#)  
[Podprogram od OpenSSH-a](#)  
[Manuelan način](#)  
[Primer podešavanja za OpenSSH](#)  
[Možete koristiti root nalog za OpenSSH](#)

[SSH Tunnel](#)  
[Upotreba OpenSSH-a](#)  
[Na početak](#)

## Primer podešavanja za [OpenSSH](#)

Globalna podešavanja za OpenSSH

/etc/ssh/ssh\_config

/etc/ssh/sshd\_config

Možete imati lične konfiguracije za različite Servere u Vašem korisničkom direktorijumu, da ne morate uvek unositi pune komande.

To će Vam olakšati logovanja i alias-e. Koristim kod svih korisnika koji imaju prava da koriste [SSH](#).

## Fajla ~/.ssh/config

U njoj podešavate kako da se ulogujete na druge kompjutere.

Kad ovu fajlu podesite možete onda koristit za logovanje

**slogin server-ime**

<http://upc.lbl.gov/docs/user/sshagent.html>

~/.ssh/config

```
# Options for all Servers
Host *
    Protocol 2
    Compression no
    ForwardAgent yes
    ForwardX11 yes
    ForwardX11Trusted yes
```

```
#PasswordAuthentication yes
```

....

Host server-ime

```
HostName      192.168.2.2
User          Vaš-korisnik ili korisnik za logovanja
Port          *****
IdentityFile   ~/.ssh/privat_dsa
PasswordAuthentication no
```

Host server-imep

```
HostName      192.168.2.2
User          Vaš-korisnik ili korisnik za logovanja
Port          *****
IdentityFile   ~/.ssh/id_dsa
PasswordAuthentication no
```

....

Možete koristiti ovu skriptu da se može kopirati od [korisnika za logovanja](#) njegova  
~/ssh/config koja se jedino podešava kod drugih [korisnika](#), tako da svi imaju isto što je  
veoma poželjno, dok je [~/ssh/authorized\\_keys](#) kod svih [korisnika](#) različita.

Na svim lokalnim i kompjuterima u mreži je poželjno da je ista ~/ssh/config. :D

/home/bin/ssh-config

## Fajla ~/ssh/authorized\_keys

U njoj podešavate ko sme da se uloguje na Vaš kompjuter

Pogledajte da bi razumeli ova veoma važna podešavanja

odeljak AUTHORIZED\_KEYS FILE FORMAT

**man sshd**

odeljak PATTERNS

## **man ssh\_config**

~/.ssh/authorized\_keys

```
# hostname, korisnik
# privat_dsa
ssh-dss ...== korisnik@hostname
# id_dsa
ssh-dss ...== korisnik@hostname
...
```

Ako hoćete da ograničite da korisnik odmah starta **tmux** sesiju i da Vi možete sve da kontrolišete šta on radi. Čim se tmux napusti odmah se korisnik izloguje.

```
command="tmux attach || tmux" ssh-dss ... korisnik@hostname
```

## **SSH Tunnel**

<http://mywiki.wooleedge.org/CategorySsh>

[http://wiki.shellium.org/w/How\\_to\\_ssh\\_tunnel](http://wiki.shellium.org/w/How_to_ssh_tunnel)

[http://hea-www.harvard.edu/~fine/OSX/afp\\_tunneling.html](http://hea-www.harvard.edu/~fine/OSX/afp_tunneling.html)

<http://dailypackage.fedorabook.com/index.php?/archives/48-Wednesday-Why-Trusted-and-Untrusted-X11-Forwarding-with-SSH.html>

**Kad je jednom napravljen SSH Tunnel on se može skoro uvek koristiti.**

**Čak iako se Server restartuje, ako je podešen Autossh, onda se restartuje automatski SSH tunel u određenom vremenu. Što je odlično.**

Možete to na više načina uraditi

Na primer za VNC protokol, pogledajte Da bi mogli koristiti SSH Tunnel sa VNC

```
ssh -p Viši-port druge-opcije -L 12022:192.168.1.4:5900 localhost
```

```
ssh -p Viši-port druge-opcije -L 12022:Vaš-udaljeni-host:5900 localhost
```

Ako nećete nikakvu komandu da izvršite na udaljenom host-u možete koristiti **-N** opciju, da se samo napravi [SSH Tunnel](#) i ništa više.

Ako hoćete da koristite grafičke programe možete da koristite opciju **-Y**, koja kaže da verujete toj drugoj strani. Oprezno sa tom opcijom.

Ako koristite **-X** opciju, to znači da ne verujete drugoj strani i možete dobiti nešto slično

Warning: untrusted X11 forwarding setup failed: xauth key data not generated

Warning: No xauth data; using fake authentication data for X11 forwarding.

Možete proveriti da li imate [SSH Tunnel](#) i da li se koristi na primer sa

**netstat -an | grep IP-adresa**

[SSH Tunnel](#) možete ubiti ako znate koji je proces sa

`kill ssh-tunnel-proses-pid`

ili jednostavno napustite određeni proces, valjda znate šta ste pokrenuli.

Možete ubiti sve [OpenSSH](#) procese sa

`killall sshd`

Možda ćete morati da se izlogujete, da bi se potpuno prekinuli svi [SSH Tunnel](#) procesi.

Odmah ponovo podignite, jer ga sigurno trebate, [OpenSSH](#) sa

Za [BSD](#)

`/etc/rc.d/sshd start`

Za [GNU/Linux](#)

`/etc/init.d/sshd start`

## **Upotreba OpenSSH-a**

Pogledajte [Kako da ubijete neželjenog ubiti SSH korisnika, Možete koristiti Tar i SSH u istom koraku.](#)

Preporučujem Vam da ako koristite [XTerm](#) da startate više sesija za [rxvt-unicode](#) da startate više tabova.

Koristite svaki tab za posebne sesije za logovanje na različite kompjutere. Tu trebate onda da date šifre za [SSH ključeve](#), da ih ne morate svaki put unositi, kad koristite [Rsync](#) ili scp. Onda možete neke tabove koristiti za povratne veze na Vaš kompjuter a u ostalima možete u svakom tabu startati [tmux](#) sesije koje su potpuno nezavisne.

Kako da blokirate za [BSD](#) sa [zaštitnim zidom](#)

[http://www.freebsdwiki.net/index.php/Block\\_repeated\\_illegal\\_or\\_failed\\_SSH\\_logins](http://www.freebsdwiki.net/index.php/Block_repeated_illegal_or_failed_SSH_logins)

Koja dobra pravila trebate da koristite

<http://lackof.org/taggart/hacking/ssh/>

Transparent Multi-hop [SSH](#)

Možete i da preskačete malo po netu Vaše Hostove

[http://linuxnet.ch/groups/linuxnet/wiki/55fd6/SSH\\_Transparent\\_Multihop\\_SSH.html](http://linuxnet.ch/groups/linuxnet/wiki/55fd6/SSH_Transparent_Multihop_SSH.html)

Kako da se kopirate sa [SSH](#)

<http://linuxtipsandtricks-jacki.blogspot.com/2009/05/how-to-copy-files-across.html>

Da vidite koje ste portove dali za [SSH](#)

```
netstat -l --tcp -p|grep ssh
```

Ako ne možete da se ulogujete na Server onda na njemu uradite debug [SSH-a](#)

```
sshd -ddd
```

Dodajte u /etc/groups neku grupu za logovanja i dodelite [korisnika za logovanja](#) u nju. I tu grupu navesti kao dozvoljenu grupu. To je još sigurnije.

Kad se prebacuje sa kompjutera na kompjuter nešto, onda je najbolje kao [root](#) zapakovati, jer on ima sva prava i može sve zapakovati, to jest pročitati.

A ako se šalju pojedine fajle onda može da se desi da se naši znakovi i delimično prava u njima izgube, korisnik ne može nešto pročitati...

## Obaveštenja prilikom [SSH](#) logovanja na Vaš kompjuter

Ako hoćete da imate zvukove i [grafička obaveštenja](#) prilikom logovanja na Vaš kompjuter, treba da podesite na primer

Napravite fajlu kao [root](#) i podesite prava

```
touch /home/log
```

```
chmod 660 /home/log
```

Proverite kako sad izgleda

```
ls -lh /home/log
```

Za [BSD](#)

```
-rw-rw---- 1 root wheel datum /home/log
```

Za [GNU/Linux](#)

```
-rw-rw---- 1 korisnik users datum /home/log
```

Stavite u konfiguracione fajle za [Shell](#) Vašeg [korisnika za logovanja](#)

Za [tcsh](#)

.cshrc

Za [Bash](#)

.bashrc

```
# OpenSSH Stuff  
echo 1 > /home/log  
mplayer-sound DoorOpen
```

Ovu skriptu najbolje je da pokrenete preko [~/.xinitrc](#) od [normalnog korisnika](#), jer onda se samo jednom pokreće pri startanju [X-a](#)

```
/home/bin/ssh-logovanje
```

Odsada kad god se neko kod Vas uloguje a to dajte samo preko Vašeg [korisnika za logovanja](#) čućete muziku i videćete grafičku poruku preko [obaveštenja za X](#).

## Logovanje preko SSH-a

**Za početak zbog jednostavnosti, možemo još da koristimo [root](#) za ssh prenos.**

**Ali kasnije ne koristite [root](#)-a za ssh prenos ni u kom slučaju, nije to uputno i bolje je da se izbegava to jest zabrani, jer je veoma nesigurno.**

**Bolje je kao [root](#) zapakovati i kao user prebaciti gde treba.**

Podesiti na oba kompjutera (prvo osigurati), ako hoćete da se koristi neki drugi Port a ne default 22, na primer Port xxxx. Za sad možete ostaviti default.

```
/etc/ssh/ssh_config
```

```
/etc/ssh/sshd_config
```

Za [BSD](#)

```
/etc/rc.d/sshd restart
```

Za [GNU/Linux](#)

```
/etc/init.d/sshd restart
```

Vidite prvo koju internu adresu imate na oba kompjutera sa

```
ifconfig | grep "inet addr"
```

ili

```
ifconfig | grep "inet addr"
```

Zavisi od konfiguracije Vašeg Modema ili Router-a koju internu adresu dobijate  
Adrese mogu biti biti u opsezima

192.168.1.  
192.168.0.  
10.0.

Zapišite na papir te interne adrese trebaće Vam to više puta.

Ulogujte se preko shell-a na system koji je podignut  
pomoću Vašeg [Live CD-a](#) sa

Kod dinamičke veze

```
ssh -p 22 root@192.168.x.yz
```

Kod statične veze

```
ssh -p 22 root@10.0.x.yz
```

Preko [Internet](#) veze

```
ssh -p 22 root@xxx.xxx.xxx.xx
```

U [Midnight Commander](#)-u sa "Shell link"

```
root@192.168.x.yz -p 22
```

Ako hoćete da kopirate fajle ili koristite za to scp

Kopirate sa Vašeg kompjutera sa Vašeg [Live CD](#)

Ako se na Vašem kompjuteru nalazite sa

```
scp -P 22 /gde/je/fajla root@192.168.x.yz:/mnt/gentoo/gde/kopirate
```

Ako se nalazite na Vašem [Live CD](#) sa

```
scp -P 22 root@192.168.x.yz:/gde/je/fajla /mnt/gentoo/gde/kopirate
```

Kopirate sa Vašeg [Live CD](#)-a na Vaš kompjuter

Ako se na Vašem kompjuteru nalazite sa

```
scp -P 22 root@192.168.x.yz:/mnt/gentoo/gde/je/fajla /gde/kopirate
```

Ako se na nalazite na Vašem [Live CD](#) sa

```
scp -P 22 /mnt/gentoo/gde/je/fajla root@192.168.x.yz:/gde/kopirate
```

Tako se mogu prebacivati podešavanja i velika je pomoć za sve ostalo.

[Podesite sada Vaš /etc direktorijum, to je najvažnije u svakom UNIX-like sistemu.](#)

Performing UDP tunneling through an SSH connection

<http://zarb.org/~gc/html/udp-in-ssh-tunneling.html>

Najbolje uđite u /podaci/Razmena ili dajte komandu

```
su  
tar cfvjP /podaci/Razmena/neki-paket.tar.bz2 /nešto/što/treba/
```

Mada možete i

```
cd /podaci/Razmena
```

```
tar cfvjP neki-paket.tar.bz2 /nešto/što/treba/
```

onda dopustiti da korisnik za logovanja može da koristi datu fajlu

```
chown korisnik-za-logovanja:wheel neki-paket.tar.bz2
```

```
exit
```

ili za direktorijume sve odjednom

Jer samo root može važne fajle u /etc/ itd. da pakuje pošto ima absolutna prava

```
su
```

```
/home/bin/ssh-virtual
```

Izlogujte se kao root

```
exit
```

Ako ste na drugom kompjuteru napravili nekog korisnika za logovanja i odradili sve što je gore napisano, onda je lako, jer isti korisnik postoji i tamo sa istim pravim i UID 555, pa mu automatski sve pripada.

```
su korisnik-za-logovanja
```

```
scp -P xxxx /podaci/Razmena/neki-paket.tar.bz2 korisnik-za-logovanja@192.168.1.35:/podaci/Razmena/
```

ili

```
cd /podaci/Razmena
```

```
scp -P xxxx ./neki-paket.tar.bz2 neki-korisnik-za-  
logovanja@192.168.1.35:/podaci/Razmena/
```

Možete proveriti šta vidi [SSH](#) na Serveru

```
ssh server uname -a
```

Probajte za debug, testfile mora da bude prazna

```
ssh server true > testfile
```

```
ls -l testfile
```

```
-rw-r--r-- 1 korisnik grupa 0 datum testfile
```

**Možete ovo uraditi ali je najsigurnije da za [SSH](#) prenos koristite samo korisnika za logovanje bez puno prava!**

A ako hoćete neku fajlu bez [root](#)-a da kopirate, koja Vama kao normalnom korisniku pripada i taj korisnik sa istim UID 500 npr. postoji na drugom kompjuteru.

Ako nije isti UID ide isto, samo što onda mora root da promeni prava i korisnika fajle.

U [GNU/Linux](#)-u nije važno ime nego UID to jest broj korisnika. na primer na A je korisnik vlada UID 500, na B jovan UID 500. Kad vlada pošalje jovan-u fajlu ona automatski pripada jovan-u kad dođe na njegov kompjuter.

Ako se već niste kao normalni korisnik ulogovali, ali ste to sigurno već uradili.

Normalno za ovo morate dopustiti da se ulogujete kao [normalni korisnik](#) u [/etc/ssh/sshd\\_config](#)

```
su vlada
```

```
scp -P xxxx " /podaci/Tekstovi/Podesavanja/Uputstvo/Instalacija GNU Linux-a.pdf" \  
jovan@192.168.1.35:/podaci/Tekstovi/Podesavanja/Uputstvo/
```

Da prenesete distfiles a da sačuvate datum i prava

```
scp -rp /usr/ports/distfiles/ server3:/usr/ports/
```

Da prenesete packages a da sačuvate datum i prava

```
scp -rp /usr/ports/packages/ server3:/usr/ports/
```

**Ako instalirate radite dalje prema [Portage](#).**

**Možete koristiti [root](#) nalog za [OpenSSH](#)**

**Napravite [ključeve za OpenSSH](#) za [root-a](#) i [razmenite ih](#) sasvim normalno**

**Morate imati podešene [ključeve za OpenSSH](#), da ne koristite šifre za [SSH](#) logovanja, što je veoma bitno za sigurnost.**

Jedina razlika je što je bolje da ključeve tačno nazovete da se odmah vidi da nisu obični

```
/root/.ssh/privat_dsa
```

**Potrebno je da ograničite korišćenje [root](#) naloga za [OpenSSH](#)**

```
/etc/ssh/sshd_config
```

```
# Very secure, don't change Order, needed for restricted Rsync and tmux
# Don't use to allow root logins, If You have only root and no users in Emulators (KVM,
VirtualBox)
```

**Ovaj raspored je veoma bitan, po ovom redu napišite!**

Sa ovim dopuštate da se root uloguje, ali samo sa SSH ključevima, uputno i za emulatore (KVM, VirtualBox)

### **PermitRootLogin without-password**

Dopuštate da se root uloguje, ali samo da izvrši određenu komandu

### **PermitRootLogin forced-commands-only**

Zabranjujete da se root uloguje sa šiframa, kao SSH korisnik, ne sme biti pre drugih opcija.

### **PermitRootLogin no**

Naravno morate da dopustite da se mogu root i njegova grupa ulogovati.

Preporučujem da u svakom slučaju ograničite sa kojih IP adresa se može root ulogovati, na primer sve adrese u rangu 192.168.1.\* su dozvoljene i ništa više

### **/root/.ssh/authorized\_keys**

**from="192.168.1.?" ssh-dss ...**

Možete koristiti root nalog za OpenSSH samo za restriktivni Rsync

Veoma je bitno da podesite, da bi mogli koristiti razne opcije kod Rsync komande, poželjno je da ograničite koji direktorijum se sme koristiti.

**command="/usr/local/bin/rsync /direktorijum" ssh-dss SSH-ključ root@host**

Da ograničite IP adrese sa kojih može da se root uloguje i koristite Rsync komande

**from="192.168.1.?",command="/usr/local/bin/rsync /direktorijum" ssh-dss ...**

SSH Protokol

OpenSSH

Dodatni programi za SSH protokol

[Ključevi za OpenSSH](#)

[Primer podešavanja za OpenSSH](#)

[SSH Tunnel](#)

[Upotreba OpenSSH-a](#)

[Možete koristiti root nalog za OpenSSH](#)

[Na početak](#)

## **FUSE, Filesystem in Userspace**

Da vidite šta ima

Za [BSD](#)

```
find /usr/ports/* | grep fusefs
```

Za [GNU/Linux](#)

```
eix fuse
```

```
eix -S fuse
```

Morate imati u [GNU/Linux Kernel](#)-u podršku za [FUSE](#)

```
zgrep FUSE /proc/config.gz
```

```
CONFIG_FUSE_FS=m
```

## **FUSE**

An interface for filesystems implemented in userspace.

<http://fuse.sourceforge.net/>

Za [BSD](#)

```
portmaster -n sysutils/fusefs-libs
```

Za [GNU/Linux](#)

```
emerge -a sys-fs/fuse
```

FUSE se može koristiti na puno načina

[http://en.gentoo-wiki.com/wiki/Mounting\\_SFTP\\_and\\_FTP\\_shares](http://en.gentoo-wiki.com/wiki/Mounting_SFTP_and_FTP_shares)

Možete particije kriptovati pomoću EncFS, automatski mountovati sa Afuse.

## **SSHFS, SSH Filesystem**

Fuse-filesystem utilizing the sftp service.

SSHFS allows you to mount a remote directory over a normal ssh connection.

<http://fuse.sourceforge.net/sshfs.html>

Za BSD

```
portmaster -n sysutils/fusefs-sshfs
```

Za GNU/Linux

```
emerge -a sshfs-fuse
```

```
sshfs --help
```

```
man sshfs
```

<https://help.ubuntu.com/community/SSHFS>

<http://www.gentoofreunde.org/node/499>

<https://wiki.archlinux.org/index.php/Sshfs>

<http://www.linuxjournal.com/article/8904>

<http://www.bluug.org/index.php?q=node/83>

<http://www.dd-wrt.com/wiki/index.php/Sshfs>

[http://lug.rose-hulman.edu/wiki/HOWTO\\_Use\\_sshfs\\_to\\_mount\\_AFS/DFS\\_home](http://lug.rose-hulman.edu/wiki/HOWTO_Use_sshfs_to_mount_AFS/DFS_home)

Da bi mogli kao korisnik da mountujete podesite

Za [GNU/Linux](#)

/etc/fuse.conf

user\_allow\_other

Možete mountovati, ako je podešeno da se logujete sa [OpenSSH ključevima](#),  
dopušta se i da [root](#) vidi taj direktorijum, jednostavno sa

```
sshfs -o allow_root host:/podaci/Razmena/SSHFS /podaci/Razmena/SSHFS
```

Možete umountovati sa

```
fusermount -u /podaci/Razmena/SSHFS
```

Za lakše mountovanje tog direktorijuma možete podestiti

```
~/.bashrc
```

Da vidite šta je podignuto za [SSHFS](#)

```
ps auxw | grep sshfs
```

## SMBNetFS

Is a filesystem that allow you to use [Samba](#) microsoft network in the same manner as the network neighborhood in Microsoft Windows.

<http://sourceforge.net/projects/smbnetfs/>

Za [BSD](#)

```
portmaster -n sysutils/fusefs-smbnetfs
```

## SMB for Fuse

Instead of mounting one [Samba](#) share at a time, you mount all workgroups, hosts and shares at once.

<http://www.ricardis.tudelft.nl/~vincent/fusesmb/>

Za [GNU/Linux](#)

```
emerge -a fusesmb
```

```
man fusesmb
```

```
man fusesmb.conf
```

```
fusesmb --help
```

Mora da postoji, ili neće [SMB for Fuse](#) moći da starta

```
~/.smb/fusesmb.conf
```

Imate primer pa samo kopirajte i promenite sa na primer

```
mkdir ~/.smb
```

```
cp -a /usr/share/doc/fusesmb*/fusesmb.conf.ex ~/.smb/smb.conf
```

[Na početak](#)

## Šifrovanje i upotreba GNU Privacy Guard-a, zamena za PGP

### Kratka istorija GnuPG

<http://lists.gnupg.org/pipermail/gnupg-announce/2007q4/000268.html>

[http://dewinter.com/gnupg\\_howto/english/GPGMiniHowto.html](http://dewinter.com/gnupg_howto/english/GPGMiniHowto.html)

<http://www.fredshack.com/docs/pgp.html>

<http://www.gentoo.org/doc/en/gnupg-user.xml>

## Programi za GnuPG

### GnuPG, The GNU Privacy Guard

Is a complete and free replacement for PGP.

Because it does not use the patented IDEA algorithm, it can be used without any restrictions. GnuPG is an RFC2440 (OpenPGP) compliant application.

<http://www.gnupg.org>

Za [BSD](#)

```
portmaster -n security/gnupg security/libgpg-error security/gpgme
```

Za [GNU/Linux](#)

```
emerge -a gnupg libgpg-error gpgme
```

Za [Mac OS X](#)

### PGPTools

Is a toolbox of a variety of programs and services to easily encrypt/decrypt and sign/verify files and e-mails on your Mac.

<http://macgpg.sourceforge.net/>

<http://www.gpgtools.org/>

GnuPG je odličan za [kriptovanje fajli](#), [elektronsku poštu](#), [Instant Messaging](#).

## Pinentry

This is a collection of simple PIN or passphrase entry dialogs which utilize the Assuan protocol as described by the aegypten project.

<http://www.gnupg.org/aegypten2/>

Za [BSD](#)

```
portmaster -n security/pinentry
```

Za [GNU/Linux](#)

```
emerge -a pinentry
```

Možete koristiti [Pinentry](#), da bi se Vaše šifre pamtile u memoriji, da ne bi morali stalno da ih pišete. Naravno treba da navedete koji ključ koristite u samim programima.

Izaberite koji ćete [Pinentry](#) program koristiti u podešavanjima za [GnuPG](#).

## [\*\*GUI za GnuPG\*\*](#)

[http://www.gnupg.org/related\\_software/frontends.en.html](http://www.gnupg.org/related_software/frontends.en.html)

## **GPA, GNU Privacy Assistant**

The GNU Privacy Assistant (GPA) is a graphical user interface for [GnuPG](#)

The GNU Privacy Assistant is a graphical frontend to [GnuPG](#) and may be used to manage the keys and encrypt/decrypt/sign/check files. It is much like [Seahorse](#).

Standardni Gnu Privacy Assistant, ima i za [smopu!M](#). Odlično radi.  
Preporučujem kombinaciju [Seahorse](#) i [GPA, GNU Privacy Assistant](#).

[http://www.gnupg.org/related\\_software/gpa/](http://www.gnupg.org/related_software/gpa/)

<http://gpa.wald.intevation.org>

Za [\*\*BSD\*\*](#)

```
portmaster -n security/gpa
```

Za [GNU/Linux](#)

```
emerge -a gpa
```

## **Seahorse**

Is a [Gnome](#) front end for [GnuPG](#). It is a tool for secure communications and data storage. Data encryption and digital signature creation can easily be performed through a GUI and Key Management operations can easily be carried out through an intuitive interface.

Odlično radi. Preporučujem kombinaciju [Seahorse](#) i [GPA, GNU Privacy Assistant](#).

<http://www.gnome.org/projects/seahorse/index.html>

Za [BSD](#)

```
portmaster -n security/seahorse
```

Za [GNU/Linux](#)

```
emerge -a seahorse
```

Dodatne opcije za [Seahorse](#), preporučujem da ih instalirate.

Za [BSD](#)

```
portmaster -n security/seahorse-plugins
```

Za [GNU/Linux](#)

```
emerge -a seahorse-plugins
```

## GnuPG-Interface

Is a Perl module interface to interacting with [GnuPG](#).

<http://search.cpan.org/dist/GnuPG-Interface/>

Za [BSD](#)

```
portmaster -n security/p5-GnuPG-Interface
```

Za [GNU/Linux](#)

```
emerge -a GnuPG-Interface
```

## **Kgpg**

[KDE](#) gpg keyring manager

[KDE](#) program za manipulisanje ključevima.

Za [BSD](#)

```
portmaster -n security/kgpg
```

Za [GNU/Linux](#)

```
emerge -a kgpg
```

## **gpg-ringmgr**

[Gentoo](#) program ([konzolni](#), Perl)

```
emerge -a gpg-ringmgr
```

## **GnuPG Shell**

Samo shell za komandni originalni program

<http://www.tech-faq.com/gnupg-shell.shtml>

## **GnuPG za Windows**

Koristite isto [GnuPG](#), ima binaries ili prevedite

## **GnuPG for Windows**

Sadrži [GnuPG](#), [WinPT](#), [GPA](#), [GPGol](#), [GPGee](#), [Claws Mail](#)...

Proverite uvek da li ima novijih verzija koje bolje rade, na ovoj stranici imate linkove

<http://www.gpg4win.org/>

## **WinPT**

Ne razvija se više, bolje je da koristite [GnuPG for Windows.](#)

<http://wald.intevation.org/projects/winpt/>

## **GPGol, GNU Privacy Guard Microsoft Outlook**

Nije potrebno, jer Outlook ne treba koristiti, mnogo sigurniji i bolji je [Claws Mail](#)

<http://www.claws-mail.org/win32/index.php>

<http://www.g10code.de/p-gpgol.html>

## **GP Gee, GNU Privacy Guard Explorer Extension**

<http://gpgee.excelcia.org/>

## **Prevođenje sa MinGW**

Ako hoćete da prevedete najnovije originalne Source od GnuPG-a

<http://clbianco.altervista.org/gnupg/eng/gnupg.html>

[Šifrovanje i upotreba GNU Privacy Guard-a, zamena za PGP](#)

[Kratka istorija GnuPG](#)

[Programi za GnupG](#)

[GnuPG The GNU Privacy Guard](#)

[Opširna lista koji sve GUI postoje za GnuPG](#)

[Seahorse](#)

[GnuPG-Interface](#)

[Kpgp](#)

[GPA, GNU Privacy Assistant](#)

[gpg-ringmgr](#)

[GnuPG Shell](#)

[GnuPG za Windows](#)

[GnuPG for Windows](#)

[WinPT](#)

[GPGol, GNU Privacy Guard Microsoft Outlook](#)

[GP Gee, GNU Privacy Guard Explorer Extension](#)

[Prevođenje sa MinGW](#)

[Uputstva kako koristiti GnuPG za GNU/Linux i Windows](#)

[Ključevi za GnuPG](#)

[Razne ostale komande sa rad sa GnuPG-om](#)

[Da bi GnuPG-Agent radio u konzoli i u X-u](#)

[Na početak](#)

## **Uputstva kako koristiti GnuPG za BSD, GNU/Linux i Windows**

Dobro pročitajte nije uputno samo za smopu!M nego i za BSD i GNU/Linux

<http://www.gnupg.org/documentation/manuals/gnupg/Operational-GPG-Commands.html>

<http://www.gpg4win.org/handbuecher/novices.html>

<http://www.gpg4win.org/handbuecher/durchblicker.html>

<http://www.coresecure.com/v5/gnupg.html>

<http://www.techmalaya.com/2008/06/17/encrypt-emails-gnupg-gpg-winpt/>

<http://www.vigay.com/security/gpg-windows.html>

<http://enigmail.mozdev.org/documentation/gpgsetup.php>

<http://www.ubuntu.ba/sistem/sigurnost/15-uvod-u-gnupg>

<http://www.gentoo.org/doc/en/gnupg-user.xml>

<http://www.gentoo.org/doc/de/gnupg-user.xml>

Možete podesiti Vašu konfiguraciju za gpg-agent

<http://www.gnupg.org/documentation/manuals/gnupg/Agent-Options.html>

<http://wiki.ubuntuusers.de/GPG-Agent>

~/.gnupg/gpg-agent.conf

Pošaljite probno potpisano pismo sa elektronskom poštom ili poruku sa Instant Messaging ili na neki drugi način sa dodatkom Vašeg javnog GnuPG ključa željenom pošiljaocu.

Kad on Vama isto pošalje njegov javni GnuPG ključem, sačuvajte ga i možete ga uvesti u Vašu listu GnuPG ključeva

Probajte da mu pošaljete nešto šifrovano sa GnuPG, takođe i on Vama.

Ako je sve u redu i možete jedno drugom da pročitate šta ste napisali, onda ste uspeli.

Od sad možete biti sigurniji, jer niko ne može pročitati više prepisku, ako razmenujete šifrovano.

## Ključevi za GnuPG

Pogledajte šta da radite dok pravite ključeve.

### Pravljenje ključeva za GnuPG preko konzole

<http://www.pps.jussieu.fr/~jch/software/pgp-validating.html>

<http://my.opera.com/mulander/blog/show.dml/427857>

Napravite ključ DSA Elgamail 4096 Bita prema datoj stranici

#### **gpg --help**

```
gpg --gen-key  
gpg --list-keys  
gpg --list-secret-keys  
gpg --list-sigs  
gpg -a --output Vaš.asc --export Vaša-email@adresa
```

### Pravljenje ključeva za GnuPG preko GUI-a

Preporučujem da koristite [Seahorse](#) i [GPA](#).

Mada možete svaki [GUI](#) koristiti.

[Vidite listu GUI programa koji podržavaju GnuPG.](#)

Sa [GPA](#)

Keys / New key ili CTRL + N

Sa [Seahorse](#)

File / New ili CTRL + N / PGP Key

Izaberite PGP Key

Napišite Vaše podatke

Ime i prezime

Adresa elektronske pošte

Comment nije obavezan

Uključite dodatne opcije i izaberite

Encryption Type

RSA

ili

DSA Elgamil

Key Strength (bits)

najveća jačina 4096

Expiration Date

Never expires uključiti, znači ne ističe nikad

Create

da napravite ključ, dajte šifru kojom zaštićujete taj ključ i dobro je zapamtite i zapišite

**Posle ne zaboravite da izvezete Vaš kompletan ključ, u kome je i Vaš tajni ključ i da ga zapamite na neko dobro čuvano mesto, USB, CD-Rom...**

**Samo ni slučajno u ~, vaš lični direktorijum (/home/user).**

Izvezite Vaš tajni ključ na primer sa

Sa [GPA](#)

Key Manager / Keys / desni klik na Vaš ključ / Backup

Sa [Seahorse](#)

My Personal Keys / desni klik na Vaš ključ / Details / Export

Nazovite ga na primer da tačno znate šta je

**Prezime Ime, tajni Ključ-UID.asc**

Izvezite Vaš javni ključ na primer sa

Sa [GPA](#)

Sa [Seahorse](#)

My Personal Keys / desni klik na Vaš ključ / Export

Nazovite taj Vaš javni ključ koji treba da date drugima na primer, daćete Vaše ime samo ako želite

**nadimak, javni Ključ-UID.asc**

Isto čuvajte i javne ključeve koje sakupite, ali oni trebaju biti dostupni samo kad ih uvozite u VAŠ [GnuPG](#) keyring.

Poželjno je da imate rezervu na nekom drugom mestu, kao  
/paketi/Net/Sigurnost/GnuPG/Ključevi

Za sve operacije možete koristiti [GnuPG](#) Shell

gpg --edit-key drugi.asc

**Sve vaše ključeve zapamtite na neko sigurno mesto (CD, USB), privatni ključevi moraju da se čuvaju kao oko u glavi.**

**Može da se desi da neko skuplja Vaše šifrovane poruke godinama i kad jednom dobije ili ukrade Vaš privatni [GnuPG](#) ključ da pročita sve Vaše poruke. Dobro je da povremeno (2 do 2 godine) menjate [GnuPG](#) ključeve.**

**Preporučujem da koristite samo jedan ključ za sve Vaše potrebe, da sami sebi ne biste pravili zabunu.**

## Razmena GnuPG ključeva

**Nikad ne šaljite tajne ključeve, šaljite samo javne!**

Izvezite javne ključeve sa [GPA](#) ili [Seahorse](#), pa samo njih šaljite.

Razmenite javne ključeve preko [Jabber](#)-a ili [elektronske pošte](#), zapamtite i uvezite u Vaš Key-Ring sa

Sa [GPA](#)

Keys / Import Keys

Sa [Seahorse](#)

File / Import ili CTRL+I (veliko i)

Sa [Kgpg](#)

Ključevi / Uvezi ključ ili CTRL+V

Preko [konsole](#)

```
gpg --import drugi.asc
```

Da potpišete ključ, samo lokalno to uradite

Sa [GPA](#)

Key Manager / Key / Set Owner Trust

Key Manager / Key / Sign Keys / Sign only locally

Sa [Seahorse](#)

Other Keys / Key / Sign Key

Preko [konsole](#)

Da potpišete ključ samo lokalno

```
gpg --lsign-key drugi.asc
```

Da potpišete ključ

```
gpg --sign-key drugi.asc
```

Pazite ako potpišete nečiji javni [GnuPG](#) ključ sa Vašim starim ključem a hoćete da koristite Vaš novi [GnuPG](#) ključ, treba da izbrišete taj javni ključ iz Vaše [GnuPG](#) liste i da ga ponovo uvezete.

Programi koji mogu da koriste [GnuPG](#) ključeve su [Claws Mail](#), [Gajim](#), [Psi](#), [Mcabber](#)...

## Davanje GnuPG javnih ključeva na Server

**Ovo ne preporučujem, bolje je ne davati svoje podatke.**

Dati javni ključ na server pomoću [Seahorse](#) ili [Kgpg](#)-a.

Uvesti sa servera njegov javni ključ, dopustiti mu u [Seahorse](#) ili [Kgpg](#)-u koliko hoćete, ako ga dobro poznajete dajte mu sva ovlašćenja koja želite. Budite oprezni.

## Dodavanje identiteta u GnuPG ključ

Ako hoćete da dodate identitet u ključ, da biste mogli koristiti sa jednim ključem više Email adresa, nije obavezno potrebno.

Proverite prvo koje ključeve imate

```
gpg --list-keys
```

```
gpg --edit-key Ključ-UID
```

adduid Ime i Prezime

napišite Real Name

kad Vas pita napišite Vašu email adresu

Ako želite, nije obavezan

Comment

Ako je sve u redu "O"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?

save

Da proverite da li je vaša druga Email adresa podržana u PGP

```
gpg --list-keys
```

## **Brisanje GnuPG ključeva**

Da izbrišete (revok-ujete) Vaše ključeve

Napravite revoke zertifikat (za opozivanje ključa)

```
gpg --gen-revoke Ključ-UID > revoke.email.asc
```

ili

```
gpg --output revoke.email.asc --gen-revoke Ključ-UID
```

Da izbrišete potpis

```
gpg --edit-key delsig Ključ-UID
```

**Importujte revoke.asc za dati ključ, pažnja time ga uništavate zauvek**

```
gpg --import revoke.email.asc
```

Pošaljite ga na Server, da se i tamo povuče, samo ako ste ga poslali pre na Server.

```
gpg --send-keys Ključ-UID
```

Posle možete i lokalno u [Seahorse](#) ili [Kgpg](#) izbrisati dati ključ.

Uvek možete vratiti osiguranje sa

```
tar xfJpP datum-normalni-korisnik.tar.xz /zajedno/bsd/home/normalni-korisnik/.gnupg
```

[Šifrovanje i upotreba GNU Privacy Guard-a, zamena za PGP](#)

[Kratka istorija GnuPG](#)

[Programi za GnuPG](#)

[Uputstva kako koristiti GnuPG za GNU/Linux i Windows](#)

[Ključevi za GnuPG](#)

[Pravljenje ključeva za GnuPG preko GUI-a](#)

[Pravljenje ključeva za GnuPG preko konzole](#)

[Razmena GnuPG ključeva](#)

[Davanje javnih ključeva na Server](#)

[Dodavanje identiteta u GnuPG ključ](#)

[Brisanje GnuPG ključeva](#)

[Razne ostale komande sa rad sa GnuPG-om](#)

[Da bi GnuPG-Agent radio u konzoli i u X-u](#)

[Na početak](#)

## **Razne ostale komande sa rad sa GnuPG-om**

Ako želite da vidite da li je neko stvarna osoba

```
gpg --fingerprint
```

Da vidite potpisne

```
gpg --list-sigs
```

Proveravate koje tajne ključeve imate

```
gpg --list-secret-keys
```

Brisanje javnog ključa

```
gpg --delete-key Ključ-UID
```

Brisanje tajnog ključa, oprezno

```
gpg --delete-secret-key
```

## **Da bi GnuPG-Agent radio u konzoli i u X-u**

```
gpg-agent --help
```

Potrebno je da imate definisani varijablu, to jest da nije prazna

```
echo $GPG_AGENT_INFO
```

Normalno se ovako GnuPG-Agent starta, ima više načina

```
eval `gpg-agent --daemon`  
gpg-agent --csh --daemon --no-grab > $HOME/.gpg-agent-info  
eval `gpg-agent --csh --daemon --no-grab --write-env-file $HOME/.gpg-agent-info`  
eval `gpg-agent --csh --daemon --no-grab --write-env-file ${HOME}/.gpg-agent-info`  
echo $GPG_AGENT_INFO > $HOME/.gpg-agent-info
```

Za [konzolu](#)

Meni je to trebalo i za [Window Manager](#)-e, pošto su oni više orijentisani na [konzolu](#)

**Pokazalo se najbolje da koristite [Keychain](#), jer on pamti SSH i GnuPG ključeve.**

Dodajte kod [normalnog korisnika](#) na primer u

Za [tcsh](#)

~/.cshrc

```
source ~/.keychain/$HOST-csh-gpg
```

Za Bash

~/.bash\_profile

```
source ~/.keychain/hostname-sh-gpg
```

Ima i ovaj komplikovaniji način za Bash

```
# http://thefunkcorner.blogspot.com/2008/06/using-gnupg-agent-on-console.html
# For Bash
# Invoke GnuPG-Agent the first time we login.
# If it exists, use this:
if test -f $HOME/.gpg-agent-info && \
   kill -0 `cut -d: -f 2 $HOME/.gpg-agent-info` 2>/dev/null; then
  GPG_AGENT_INFO=`cat $HOME/.gpg-agent-info | cut -c 16-`
  GPG_TTY=`tty`
  export GPG_TTY
  export GPG_AGENT_INFO
else
# Otherwise, it either hasn't been started, or was killed:
  eval `gpg-agent --daemon --no-grab --write-env-file $HOME/.gpg-agent-info`
  GPG_TTY=`tty`
  export GPG_TTY
  export GPG_AGENT_INFO
fi
```

Pogledajte Biranje X okruženja

Ako koristite startx komandu što je normalno stavite u

~/.xinitrc ili u skriptu /home/bin/afterx

```
...
# For GnuPG, if You need in X working gpg-agent
eval "$(gpg-agent --daemon)"
...
```

## Za KDE

Možete staviti u

~/.kde/env/gpgagent.sh

```
eval "$(gpg-agent --daemon)"
```

Ako koristite KDM, GDM, XDM, SLiM, što ne preporučujem, stavite to isto u

~/.xsession

Zaštitite Vaš [GnuPG](#) direktorijum

```
chmod u+rwx,g-rwx,o-rwx ~/.gnupg
```

[Šifrovanje i upotreba GNU Privacy Guard-a, zamena za PGP](#)

[Kratka istorija GnuPG](#)

[Programi za GnuPG](#)

[GnuPG The GNU Privacy Guard](#)

[Opširna lista koji sve GUI postoje za GnuPG](#)

[Seahorse](#)

[Kpgp](#)

[GPA, GNU Privacy Assistant](#)

[gpg-ringmgr](#)

[GnuPG Shell](#)

[GnuPG za Windows](#)

[GnuPG for Windows](#)

[WinPT](#)

[GPGol, GNU Privacy Guard Microsoft Outlook](#)

[GPGee, GNU Privacy Guard Explorer Extension](#)

[Prevođenje sa MinGW](#)

[Uputstva kako koristiti GnuPG za GNU/Linux i Windows](#)

[Ključevi za GnuPG](#)

[Pravljenje ključeva za GnuPG preko GUI-a](#)

[Pravljenje ključeva za GnuPG preko konzole](#)

[Razmena GnuPG ključeva](#)

[Davanje javnih ključeva na Server](#)

[Dodavanje identiteta u GnuPG ključ](#)

[Brisanje GnuPG ključeva](#)

[Razne ostale komande sa rad sa GnuPG-om](#)

[Da bi GnuPG-Agent radio u konzoli i u X-u](#)

[Na početak](#)

# **Kako zaštititi Instant Messaging i Internet Live Conferencing**

## **Koju zaštitu za Instant Messaging koristiti**

Encrypted Session Negotiation

<http://xmpp.org/extensions/xep-0116.html>

Current Jabber OpenPGP Usage

<http://xmpp.org/extensions/xep-0027.html>

Requirements for Encrypted Sessions

<http://xmpp.org/extensions/xep-0210.html>

Cryptographic Design of Encrypted Sessions

<http://xmpp.org/extensions/xep-0188.html>

End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP)

<http://xmpp.org/rfcs/rfc3923.html>

ZRTP: Media Path Key Agreement for Secure RTP

<http://tools.ietf.org/html/draft-zimmermann-avt-zrtp-16>

<https://secure.wikimedia.org/wikipedia/en/wiki/ZRTP>

Šta sve [Gajim](#) podržava

<http://trac.gajim.org/wiki/GajimXEPSupport>

Odlična objašnjenja na nemačkom, zašto koristiti [Jabber](#) i o [OTR](#)-u

<http://www.binaryspa.de/jabber-off-the-record/>

Odličan članak na nemačkom, piše puno o [OTR](#)-u i raznim važnim stvarima o kriptografiji

<http://public.tfh-berlin.de/~s30935/off-the-record-messaging.pdf>

Mnogo je bitno da ne koristite ključeve za IM koji se mogu kad tad ukrasti, kao GnuPG ključeve.

Koristite samo ključeve koji važe u aktuelnoj sesiji.

Tako ne može niko da skuplja Vaše šifrovane poruke godinama i kad jednom dobije Vaš GnuPG ključ da pročita sve Vaše poruke.

## **OTR (Off-the-Record Messaging)**

Veoma sigurna kombinacija raznih sistema za šifrovanje.

Kod OTR (Off-the-Record Messaging) morate se identifikovati sa frazama znanih samo Vama i Vašem kontaktu da bi imali privatnu komunikaciju.

Oba kontakta moraju da postave pitanje za autentifikaciju, da bi bila uspešna OTR komunikacija.

[https://en.wikipedia.org/wiki/Off-the-Record\\_Messaging](https://en.wikipedia.org/wiki/Off-the-Record_Messaging)

[https://de.wikipedia.org/wiki/Off-the-Record\\_Messaging](https://de.wikipedia.org/wiki/Off-the-Record_Messaging)

<http://www.cypherpunks.ca/otr/>

<http://www.cypherpunks.ca/otr/otr-wpes.pdf>

<http://www.cypherpunks.ca/otr/otr-codecon.pdf>

Privacy Levels

<http://www.cypherpunks.ca/otr/help/3.2.0/levels.php?lang=en>

Authentication

<http://www.cypherpunks.ca/otr/help/authenticate.php?lang=en>

Email lista

<http://lists.cypherpunks.ca/pipermail/otr-users>

Odličan video od Ian Goldberg

<http://csclub.uwaterloo.ca/media/Off-the-Record%20Messaging:%20Useful%20Security%20and%20Privacy%20for%20IM.html>

Odlična zbirka programa za [OTR](#) na francuskom

[http://free.korben.info/index.php?title=%C3%A9curiser\\_ses\\_conversations](http://free.korben.info/index.php?title=%C3%A9curiser_ses_conversations)

[OTR](#) autentifikaciju mogu koristiti ovi programi [Pidgin](#), [Gajim](#), [Psi](#), [vacuum-im](#), [Kopete](#), [MCabber](#)

A preko i [Irssi-otr](#) imaju mogućnost i [Irssi](#), [XChat](#), [WeeChat](#), [BitlBee](#)

<http://www.cypherpunks.ca/otr/software.php>

Osnova za [OTR](#)

(OTR) Messaging allows you to have private conversations over instant messaging

<http://www.cypherpunks.ca/otr/>

<http://otr.git.sourceforge.net/git/gitweb-index.cgi>

Za [BSD](#)

portmaster -n security/libotr

Za [GNU/Linux](#)

emerge -a libotr

[Pogledajte šta da radite dok pravite ključeve za OTR.](#)

Ima i drugi način za šifrovanje sa IRC.

<http://burnachurch.com/65/fish-verschluesselt-ins-irc/>

## **End to End message Encryption**

### **PyCrypto**

This is a collection of both secure hash functions (such as MD5 and SHA), and various encryption algorithms (AES, DES, ElGamal, etc.) for Python.

<http://www.dlitz.net/software/pycrypto/>

<http://pycrypto.org>

Za BSD

portmaster -n security/py-pycrypto

Za GNU/Linux

emerge -a pycrypto

Koristi ključeve koji se svaki put generišu, što je veoma sigurno.

Može se koristiti simetrička enkripcija.

[https://secure.wikimedia.org/wikipedia/en/wiki/Random\\_number\\_generator](https://secure.wikimedia.org/wikipedia/en/wiki/Random_number_generator)

<http://bityard.blogspot.com/2010/01/symmetric-encryption-with-pycrypto-part.html>

<http://eli.thegreenplace.net/2010/06/25/aes-encryption-of-files-in-python-with-pycrypto/>

<http://encyclopedia.thefreedictionary.com/end-to-end+encryption>

## **Koju zaštitu za Internet Live Conferencing koristiti**

Ako hoćete zaštićenu vezu samo između 2 korisnika onda možete koristiti OTR, ali to ne radi stabilno.

Ako želite da ceo kanal bude zaštićen onda morate da koristite drugi način.

## **FiSH**

It is based on blowfish and is fully compatible to original 'blowcrypt' script. It supports private chat and channel encryption.

Omogućava da imate zaštitu na Vašem IRC kanalu.

Potrebno je da je instalisan MIRACL.

<http://fish.secure.la/>

Za BSD

Postoji PBI paket, posle mog predloga od 22.03.2012.

portmaster -n irc/xchat-fish

Postoji [PBI](#) paket, posle mog predloga od 22.03.2012.

portmaster -n irc/irssi-fish

Za [GNU/Linux](#)

Instališe se ručno.

<http://m.0f.se/files/>

<https://bugs.gentoo.org/193177>

<http://downloads.lexmark.com/downloads/pssd/PPD-Files-LMACO.tar.Z>

Napravite direktorijum i uđite u njega

```
mkdir -p /paketi/Net/IRC/FiSH/Source
```

```
cd /paketi/Net/IRC/FiSH/Source
```

Možete skinuti najnoviju verziju na primer sa

```
wget http://m.0f.se/files/FiSH-irssi.v1.00-RC5-source.zip
```

Forum za [FiSH](#)

<http://fish.secure.la/forum/index.php>

Mali izbor stranica za [FiSH](#)

<http://blog.bjrn.se/2009/01/proposal-for-better-irc-encryption.html>

<http://daemonkeeper.net/65/fish-verschluesselt-ins-irc>

<http://markus.viitamaki.net/2009/08/10/irssifish-guide/>

[http://mewbies.com/how\\_to\\_install\\_fish\\_for\\_irssi\\_tutorial.htm](http://mewbies.com/how_to_install_fish_for_irssi_tutorial.htm)

**[FiSH](#) upotreba**

<http://fish.secure.la/irssi/FiSH-irssi.txt>

<http://fish.secure.la/xchat/FiSH-XChat.txt>

Za sve komande važi, ako nije kanal naveden onda važi za trenutni prozor

Pokazuje tajni ključ

```
/key korisnik/#kanal
```

Da namestite tajni ključ za korisnika

```
/setkey korisnik/#kanal tajni-ključ
```

Da obrište tajni ključ za korisnika, navedite koji korisnik i kanal

```
/delkey korisnik/#kanal
```

Da pošaljete DH1080 KeyXchange korisniku.

```
/keyx korisnik
```

Da pošaljete šifrovanu poruku korisniku.

```
/msg+ korisnik/#kanal Vaša poruka
```

Da pošaljete šifrovanu notice korisniku.

```
/notice+ korisnik/#kanal Vaša notice
```

Da namestite šifrovani topic za trenutni kanal. Pazite veličina topica se smanjuje oko 60%, to nije dovoljno na primer za normalni eBay URL

/topic+ Vaš topic

Namestite da koristite Vašu šifru da zaštitite Vašu bazu ključeva na primer

~/.xchat2/blow.ini

Moraćete svaki put kad ga otvarate da date Vašu šifru kad startate modul. Ako ne koristite Vašu šifru, koristiće se default šifra, što je nesigurno. Ako samo Vi možete čitati taj direktorijum, onda je malo lakše, mada i dalje nesigurno.

/setinipw Vaša-šifra

Da se vratite nazad na default šifru Vašu bazu ključeva

/unsetinipw

U slučaju da koristite Vašu šifru za blow.ini, treba da koristitu tu komandu posle podizanja [FiSH-a](#), samo za [GNU/Linux](#) i [BSD](#)

/fishpw Vaša-šifra

Možete podići [FiSH](#) i sa ovom komandom

/load /path/xfish.so Vaša-šifra

Da uključite ili isključite [FiSH](#) enkripciju

/encrypt [< 1/y/on | 0/n/off >]

Da uključite ili isključite [FiSH](#) dekripciju

/decrypt [< 1/y/on | 0/n/off >]

Možete zaštiti Vaš IRC kanal sa [FiSH](#), svaki korisnik mora ovo da ponovi

```
setkey #kanal tajni-ključ
```

Ako u kanalu treba da pošaljete nekom novom koji nema [FiSH](#) zaštitu, čist tekst, radi i u normalnom prozoru

+p ne zaštićeni čist tekst

## MIRACL

Multiprecision Integer and Rational Arithmetic C/C++ Library

Is a Big Number Library which implements all of the primitives necessary to design Big Number Cryptography into your real-world application.

<http://www.shamus.ie/>

Za [BSD](#)

portmaster -n math/miracl

Za [GNU/Linux](#)

emerge -a miracl

## Mircryption

Is a free encryption add-on for the popular irc clients [mIRC](#) and [XChat](#).

Is an [OpenSource](#) project, consisting of a variety of interrelated addons, programs, and scripts, that provide secure encryption for internet relay chat ([irc](#)).

The center piece of [Mircryption](#) is an addon for the [mIRC](#) irc client, but [Mircryption](#) now supports several other clients (including [XChat](#)), as well as the psbnc irc bouncer and the eggdrop irc bot program.

<http://www.donationcoder.com/Software/Mouser/mircryption/index.php>

<http://mircryption.sourceforge.net/>

Za [BSD](#)

portmaster -n irc/xchat-mircryption

Za [GNU/Linux](#)

[Instališe se ručno.](#)

Kanal #mircryption na [EFnet](#)

Forum

<http://www.donationcoder.com/forum/index.php?board=13.0>

<http://voobar.follvalsch.de/mcpsx>

[Na početak](#)

## **Zaštitite Vaše šifre**

**Nije dovoljno da su Vaše šifre jake, nego i način kako se čuvaju.**

Imate mnogo načina da to uradite. Sigurno je bolje da se i one čuvaju šifrovano.

Neki pamte to u glavi, na papiru, u normalnom Office dokumentu...

Ima nekih koji pamte svoju databasu za šifre na USB-u na zaštićenoj particiji, koja ima u sebi još dve zaštićene particije sa različitim šiframa i da je samo na jednoj ta databasa zaštićena sa jednom šifrom, dok na drugoj particiji je neka databasa koja nema u sebi ništa važno i da tu particiju pokazuju ako moraju da daju šifru organima koji to traže.

Vi sami nađite način koji odgovara Vašim potrebama, to zavisi od toga koliko znate o sigurnosti i šta se dešava u svetu.

Ima različitih programa da zaštitite Vaše šifre.

Vidite šta ima sa

eix password

## **KeePassX**

Is an application for people with extremly high demands on secure personal data management.

<http://www.keepassx.org/>

emerge -a keepassx

[https://security.ngoinabox.org/en/using\\_keepass](https://security.ngoinabox.org/en/using_keepass)

## **YAPET, Yet Another Password Encryption Tool**

A Ncurses (text) based password encryption tool

<http://www.guengel.ch/myapps/yapet/>

emerge -a yapet

Nalazi se u Overlay-u Sunrise.

## **Gringotts**

Is a secure notes manager for Linux and other UNIX-like systems.

<http://gringotts.berlios.de/>

emerge -a gringotts

## **wmpasman**

Stores your passwords, and makes them available for pasting (both via the middle-click PRIMARY selection and the CLIPBOARD selection) at the click of a button. It also contains a digital clock. Access is controlled by a passphrase.

<http://sourceforge.net/projects/wmpasman/>

emerge -a wmpasman

## **Password Safe**

Simple & Secure Password Management

Password Safe was originally written by Bruce Schneier and is now run as an OpenSource

project hosted on SourceForge.

<http://www.schneier.com/passsafe.html>

<http://pwsafe.org/>

<http://passwordsafe.sourceforge.net/>

Instališe se ručno. Ima deb paketa.

Koji sve programi koriste [Password Safe](#)

<http://pwsafe.org/relatedprojects.shtml>

## **Java PasswordSafe**

This is a Java version of the [Password Safe](#) password management utility. This utility allows you to easily and securely manage multiple passwords on [GNU/Linux](#), Mac, and Windows in a format that is compatible with the original [Password Safe](#) utility.

<http://sourceforge.net/projects/jpwsafe/>

Instališe se ručno.

## **cliPSafe**

Is a command line interface ([CLI](#)) to [Password Safe](#) databases. cliPSafe only works with version 3 databases and it currently only operates in read only mode.

<http://waxandwane.org/clipsafe.html>

Instališe se ručno.

## **Gorilla**

[Password Safe](#) clone for [GNU/Linux](#). Stores passwords in secure way with [GUI](#) interface.

Binarno pa bolje ne koristiti za ovu osetljivu temu.

<http://www.fpx.de/fp/Software/Gorilla/>

emerge -a gorilla

*Kraj Password Safe*

[Na početak](#)

## **Zaštita od virusa**

Pogledajte [Virusa ima i za BSD i GNU/Linux i Zaštita od virusa za Windows.](#)

[https://en.wikipedia.org/wiki/List\\_of\\_antivirus\\_software](https://en.wikipedia.org/wiki/List_of_antivirus_software)

Da vidite šta ima

Za [BSD](#)

```
find /usr/ports/* | grep virus  
find /usr/ports/* | grep clamav  
grep -r virus /usr/ports
```

Za [GNU/Linux](#)

```
eix app-antivirus/*  
eix -S virus
```

## **ClamAV**

Clam Antivirus is command line virus scanner written entirely in C and its database is kept up to date. It also detects polymorphic viruses, scans compressed files and supported by AMaViS.

Clam AntiVirus is an [Free Software](#) (GPL) anti-virus toolkit for UNIX, designed especially for e-mail scanning on mail gateways. It provides a number of utilities including a flexible and scalable multi-threaded daemon, a command line scanner and advanced tool for automatic database updates.

<http://www.clamav.net/>

Za [BSD](#)

```
portmaster -n security/clamav
```

Za [GNU/Linux](#)

```
emerge -a clamav
```

<http://www.freebsddiary.org/virus-scanning.php>

<https://wiki.archlinux.org/index.php/Clamav>

<https://en.wikipedia.org/wiki/Clamav>

Kanal #clamav na [Freenode](#)

Da se podigne

Za [BSD](#)

```
/usr/local/etc/rc.d/clamav-clamd start
```

```
/usr/local/etc/rc.d/clamav-freshclam start
```

Za [GNU/Linux](#)

```
/etc/init.d/clamd start
```

Da se uvek starta pri podizanju sistema

Za [BSD](#)

[/etc/rc.conf](#)

```
clamav_clamd_enable="YES"  
clamav_freshclam_enable="YES"
```

Za [GNU/Linux](#)

```
rc-update add clamd default
```

Izvršne fajle su

```
clamav-config  
clambc  
clamconf
```

```
clamdtop  
clamscan  
clamdscan  
freshclam  
sigtool  
clamav-milter  
clamd
```

Podešavanja su u

/usr/local/etc/clamd.conf

/usr/local/etc/freshclam.conf

Logovi se nalaze u direktorijumu

/var/log/clamav

Da obnovite definicije, ako ne koristite freshcam daemon

```
freshclam
```

Ako nađete virusa možete ga poslati na

[www.clamav.org/sendvirus/](http://www.clamav.org/sendvirus/)

## ClamTk

Is a GUI front-end for [ClamAV](#) using gtk2-perl. It is designed to be an easy-to-use frontend for Unix systems.

Ne treba da ga koristite kao [root](#).

<http://clamtk.sourceforge.net/>

Za [BSD](#)

Postoji [PBI](#) paket.

```
portmaster -n security/clamtk
```

Za [GNU/Linux](#)

```
emerge -a clamtk
```

## ClamAV Unofficial Signatures Updater

The clamav-unofficial-sigs script provides a simple way to download, test, and update third-party signature databases provided by Sanesecurity, MSRBL, SecuriteInfo, MalwarePatrol, and OITC. The package also contains cron, logrotate, and man files.

<http://sourceforge.net/projects/unofficial-sigs/>

Za [BSD](#)

```
portmaster -n security/clamav-unofficial-sigs
```

Za [GNU/Linux](#)

```
emerge -a clamav-unofficial-sigs
```

## ClamFS

A FUSE-based user-space file system with on-access anti-virus file scanning

<http://clamfs.sourceforge.net/>

Za [GNU/Linux](#)

```
emerge -a clamfs
```

## clamd-stream-client

Small client to ask a [ClamAV](#) antivirus server if a file contain a virus.  
May be used with procmail or maildrop rules. [ClamAV](#) library is not required to be installed on the running host.

<http://sourceforge.net/projects/clamd-stream-cl/>

Za [BSD](#)

```
portmaster -n security/clamd-stream-client
```

## Za GNU/Linux

```
emerge -a clamd-stream-client
```

[Claws Mail](#) ima dodatak za [ClamAV](#).

*Kraj ClamAV*

## **AMaViS, A Mail Virus Scanner**

Scans e-mail attachments for viruses using third-party virus scanners available for UNIX environments. It resides on a UNIX (Linux) machine and looks through the attached files arriving via e-mail, generates reports when a virus is found and sets the delivery on hold.

Ne razvija se više

<http://amavis.sourceforge.net/>

## **amavisd-new**

Is a performance-enhanced daemonized version of amavis-perl

<http://www.amavis.org/>  
<http://www.ijs.si/software/amavisd/>

## Za BSD

```
portmaster -n security/amavisd-new
```

## Za GNU/Linux

```
emerge -a amavisd-new
```

<http://perlstalker.amigo.net/amavis/amavisd-new.phtml>

## **amavisd-milter**

Is a sendmail milter for [amavisd-new](#) version 2.2.0 and above which use the new AM.PDP protocol. Full amavisd-new functionality is available, including adding spam and virus information header fields, modifying Subject, adding address extensions and removing certain recipients from delivery while delivering the same message to the rest

<http://amavisd-milter.sourceforge.net/>

Za BSD

```
portmaster -n security/amavisd-milter
```

Za GNU/Linux

```
emerge -a amavisd-milter
```

## **amavis-logwatch**

Utility is an [amavisd-new](#) log parser that produces summaries, details, and statistics regarding the operation of [amavisd-new](#) (henceforth, simply called [AMaViS](#)).

<http://logreporters.sourceforge.net/>

Za BSD

```
portmaster -n mail/amavis-logwatch
```

## **amavis-stats**

is a simple [AMaViS](#) statistics generator based on rrdtool. It produces graphs of clean emails, spam emails and infected emails broken down by virus, from amavis log entries. RRD files are created and updated by a perl script run from cron. Graphs are generated by a php script and viewed with a web browser.

<http://osx.topicdesk.com/content/view/42/80/>

Za BSD

```
portmaster -n security/amavis-stats
```

*Kraj AMaViS, A Mail Virus Scanner*

## **F-PROT**

F-Prot Antivirus for BSD Workstations utilizes the renowned F-Prot Antivirus scanning

engine for primary scan but has in addition to that a system of internal heuristics devised to search for unknown viruses.

This version of F-Prot is a command line on-demand scanner.

<http://www.f-prot.com/>

Za [BSD](#)

```
portmaster -n security/f-prot
```

Za [GNU/Linux](#)

```
emerge -a f-prot
```

## Penguin Pills

Provides a graphical interface for a number of Linux command line anti-virus scanners.

<http://penguinpills.sourceforge.net/>

[Instališe se ručno.](#)

## Dazuko

A common interface across all platforms is needed for 3rd party file access control. With such an interface, focus could be redirected from OS hacking to solving real problems. The interface is here. It is called [Dazuko](#).

[http://dazuko.dnsalias.org/wiki/index.php/Main\\_Page](http://dazuko.dnsalias.org/wiki/index.php/Main_Page)

Za [BSD](#)

```
portmaster -n security/dazuko
```

[Na početak](#)

## Kriptovanje fajli

<https://www.schneier.com/blowfish.html>

[https://en.wikipedia.org/wiki/Crypt\\_%28Unix%29](https://en.wikipedia.org/wiki/Crypt_%28Unix%29)

## Kriptovanje fajli sa GnuPG

Smatram da je kriptovanje fajli sa [GnuPG](#) najsigurnije, jer kriptujete sa javnim [GnuPG](#) ključem Vašeg sagovornika.

Tražite **gnupg files** na internetu

<http://www.gnupg.org/documentation/faqs.en.html>

<http://www.gnupg.org/gph/en/manual.html#AEN111>

<http://www.somacon.com/p107.php>

<http://www.madboa.com/geek/gpg-quickstart/>

<http://blogs.techrepublic.com.com/opensource/?p=168>

<http://www.davinciplanet.com/pgp-file-encryption-using-gnupg/>

...

Možete i sa nekim specijalnim programima [šifrovati fajle](#).

Da šifrujete (encrypt) za nekog određenog korisnika sa njegovim [GnuPG ključem](#)

gpg -e -r Ključ-UID fajla

ili

gpg -r Ključ-UID --encrypt fajla

ili najbolje tako tačno kažete koja je izlazna fajla

gpg -r Ključ-UID --output fajla.gpg --encrypt fajla

Dobićete zaštićenu fajlu

fajla.gpg

Da određeni korisnik dešifruje sa svojim [GnuPG ključem](#) (decrypt)

```
gpg -r Ključ-UID --decrypt fajla.gpg
```

ili bolje

```
gpg -r Ključ-UID --output fajla --decrypt fajla.gpg
```

## **bcrypt**

Is a blowfish file encryption utility which aims for cross-platform portability.  
In addition to providing 448-bit encryption, bcrypt overwrites input files with random garbage before deletion in order to make low-level data recovery much more difficult.

<http://bcrypt.sourceforge.net/>

Za [BSD](#)

```
portmaster -n security/bcrypt
```

Za [GNU/Linux](#)

```
emerge -a bcrypt
```

```
man bcrypt
```

```
bcrypt
```

Da šifrujete (encrypt)

```
bctypt fajla
```

Da šifrujete (encrypt) a da ostane izvorna fajla

```
bctypt -r fajla
```

Da dešifrujete (decrypt), ako je nastavak .bfe onda automatski dešifruje i traži Vam šifru

bcrypt fajla.bfe

## Možete kriptovati istovremeno sa [GnuPG](#) i [bcrypt](#)

Možete ovako postupiti, malo komplikovano ali sigurno 😊

Prvo šifrujte (encrypt) sa [bcrypt](#)

bcrypt -r fajla

Onda šifrujte (encrypt) sa [GnuPG](#) za određenog korisnika

```
gpg -r Ključ-UID --output fajla.bfe.gpg --encrypt fajla.bfe
```

Dobićete ovu fajlu

fajla.bfe.gpg

Tu fajlu pošaljite Vašem određenom korisniku sigurnim putem.

Određeni korisnik treba da bi mogao dešifruje (decrypt) da ide obrnutim redom

Da dešifruje (decrypt) sa [GnuPG](#) sa svojim [GnuPG ključem](#)

```
gpg -r Ključ-UID --output fajla.bfe --decrypt fajla.bfe.gpg
```

Da dešifrujete (decrypt) sa [bcrypt](#)

bcrypt fajla.bfe

Dobićete izvornu fajlu

fajla

## **bdes**

encrypt/decrypt using the Data Encryption Standard (DES)

Za [BSD](#)

[bdes](#) se nalazi u [FreeBSD Base paketima](#).

man bdes

## **ccrypt**

Is a utility for encrypting and decrypting files and streams. It was designed to replace the standard unix crypt utility, which is notorious for using a very weak encryption algorithm. ccrypt is based on the Rijndael cipher, which is the U.S. government's chosen candidate for the [Advanced Encryption Standard](#). This cipher is believed to provide very strong security.

<http://ccrypt.sourceforge.net/>

<http://www.mathstat.dal.ca/~selinger/ccrypt/>

Za [BSD](#)

portmaster -n security/ccrypt

Za [GNU/Linux](#)

emerge -a ccrypt

man ccrypt

ccrypt --help

<http://ccrypt.sourceforge.net/faq.html>

<https://secure.wikimedia.org/wikipedia/en/wiki/Ccrypt>

Normalno je da ovako šifrujete, pitaće Vas dva puta za šifru, dobićete fajlu sa default nastavkom **.cpt**

```
ccencrypt fajla.tar.bz2
```

Normalno se ovako dešifruje, pitaće Vas jednom za šifru

```
ccdecrypt fajla.tar.bz2.cpt
```

Sa keyfile odlično za skripte, plus povremeno, ali redovno menjajte jaku šifru

Najsigurnije je da šifrujete sa keyfile, dobićete fajlu sa default nastavkom **.cpt**

```
ccencrypt --keyfile /home/bins/ccrypt.key fajla.tar.bz2
```

Da dešifrujete možete koristiti isto keyfile

```
ccdecrypt --keyfile /home/bins/ccrypt.key fajla.tar.bz2.cpt
```

## Elettra

Plausible deniable file cryptography

<https://www.winstonsmith.info/>

<http://www.winstonsmith.info/julia/elettra/>

```
emerge -a app-crypt/elettra
```

<http://www.phrack.org/issues.html?issue=65&id=6#article>

<http://wiki.ubuntuusers.de/Elettra>

[https://secure.wikimedia.org/wikipedia/en/wiki/Winston\\_Smith\\_Project](https://secure.wikimedia.org/wikipedia/en/wiki/Winston_Smith_Project)

<http://www.youtube.com/user/progettowinstonsmith>

Potrebno je da imate instalisano

Za [BSD](#)

```
portmaster -n security/mhash security/libmcrypt
```

Za [GNU/Linux](#)

```
emerge -a app-crypt/mhash dev-libs/libmcrypt
```

Za Debian Vam je verovatno dodatno potrebno

```
apt-get install cmake mcrypt libmhash2 libmhash-dev simhash libmcrypt4 libmcrypt-dev
```

elettra example

Možete [ručno instalisati](#) i [GUI](#) za [Elettra](#) kao i nju samu

```
mkdir -p /paketni/Net/Sigurnost/Elettra/Source
```

```
cd /paketni/Net/Sigurnost/Elettra/Source
```

```
wget http://www.winstonsmith.info/julia/elettra/elettra-src.tar.gz
```

```
wget http://www.winstonsmith.info/julia/elettra/elettra_gui.tar.gz
```

Otpakujte sa

```
tar xfz elettra-src.tar.gz -C ..
```

```
tar xfz elettra_gui.tar.gz -C ..
```

Prevedite na primer Elettra sa

```
cd .../elettra/src
```

```
mkdir build && cd build
```

```
cmake ..
```

```
make
```

Linkujte sa

```
In -s /paketi/Net/Sigurnost/Elettra/elettra/src/build/elettra /usr/local/bin/elettra
```

Prevedite na primer za Elettra [GUI](#) sa

```
cd .../elettra_gui  
gcc *.cpp -l. `wx-config --cxxflags --libs` -o elettra_gui
```

Linkujte sa

```
In -s /paketi/Net/Sigurnost/Elettra/elettra_gui/elettra_gui /usr/local/bin/elettra_gui
```

Vidite primere

```
elettra example
```

Ne brinite se što su kreirane šifrovane fajle sa prozvoljnim datumom, to je namerno tako da je sigurnost još veća. Ako to nećete morate Source menjati.

Mogu se fajle ručno šifrovati na primer sa

```
elettra encrypt outputfile [size increment]% plainfile[::password]
```

Na primer

```
elettra encrypt 15% fajla-.tar.bz2 fajla.tar.bz2::šifra-jaka
```

Mogu se fajle ručno dešifrovati na primer sa istom šifrom

```
elettra decrypt cipherfile [password] [output directory]
```

Na primer

```
elettra decrypt fajla-.tar.bz2 šifra-jaka
```

Da više fajli šifrujete sa različitim šiframa

```
elettra encrypt /dev/shm/output 15% /tmp/ls-manpage::weirdness /tmp/ps-manpage::xYZ1shower
```

Na primer

```
elettra encrypt fajla-tar.bz2 15% fajla1.tar.bz2::šifra1 fajla2.tar.bz2::šifra2
```

Onda ako hoćete samo jednu fajlu da otpakujete

```
elettra decrypt /dev/shm/output weirdness /dev/shm/
```

Na primer prvu fajlu

```
elettra decrypt fajla-tar.bz2 šifra1
```

Na primer drugu fajlu

```
elettra decrypt fajla-tar.bz2 šifra2
```

Ako dobijate ovo, onda nešto niste dobro uradili ili ime fajle ili šifra nije dobra

```
invalid password or invalid file, I didn't find any valid key header
```

Da proverite da li je vaša šifra dobra, pogledajte [Šifre moraju biti veoma jake](#), ili slično da dobijete ako je u redu

```
elettra checkpass password(s)
```

password(s) combinations work ok, atleast with password block of 1280 bytes

A ako nije u redu to jest ako je kratka šifra, pazite što jača šifra to bolje

Invalid password, required 6 bytes

Fajle možete i sa standardnim programom GnuPG šifrovati.

Na početak

## **Cryptographic hash function**

[https://en.wikipedia.org/wiki/Cryptographic\\_hash\\_function](https://en.wikipedia.org/wiki/Cryptographic_hash_function)

<https://en.wikipedia.org/wiki/Md5>

### **md5**

The md5, sha1, sha256 and rmd160 utilities take as input a message of arbitrary length and produce as output a “fingerprint” or “message digest” of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5, SHA-1, SHA-256 and RIPEMD-160 algorithms are intended for digital signature applications, where a large file must be “compressed” in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

Za [BSD](#)

[md5](#) se nalazi u [FreeBSD Base paketima](#).

man md5

### **md5sum**

Compute and check MD5 message digest

Za [GNU/Linux](#)

md5sum se nalazi u paketu Coreutils.

```
man md5sum
```

## **md5deep**

Is a set of programs to compute MD5, SHA-1, SHA-256, Tiger, or Whirlpool

<http://md5deep.sourceforge.net/>

Za BSD

```
portmaster -n security/md5deep
```

Za GNU/Linux

```
emerge -a md5deep
```

## **Isomd5sum**

Is a collection of utilities for implanting and checking MD5 checksums within an ISO9660 image.

<https://fedorahosted.org/releases/i/s/isomd5sum/>

Za BSD

```
portmaster -n sysutils/isomd5sum
```

Na početak

## **Steganografija**

<http://en.wikipedia.org/wiki/Steganography>

## **Steghide**

Is a steganography tool which is able to hide data in "container files" and to extract this data again.

<http://steghide.sourceforge.net/>

Za [BSD](#)

```
portmaster -n security/steghide
```

Za [GNU/Linux](#)

```
emerge -a steghide
```

## **SSH, Kernel, Iptables, patch-o-matic**

Može se i dodati u [GNU/Linux Kernel](#) i Iptables opcija da se može samo iz određenih zemalja ulogovati preko SSH protokola, što veoma povećava sigurnost.

Ne radi trenutno sa novijim [GNU/Linux Kernel](#)-ima od 2.6.27

Zamena za patch-o-matic je [Xtables-addons](#) koji se uspešno instalira u 9999 verziji.

**Ova pačovanja više nisu potrebna.**

Sklonio sam sve skripte pošto ih više ne koristim u

```
/home/bin/kernel/iptables
```

**Iptables se mora obnoviti pre bilo kakvog patch-ovanja**

```
/home/bin/svn/svnupsve
```

Obnovite Iptables patch-o-matic (dodatke) sa

```
/home/bin/kernel/iptables-obnovi
```

Proveriti koja Iptables verzija će se sa instalisati sa

eix iptables

Kopirajte iz, da bi runme prihvatio da patch-uje [GNU/Linux Kernel](#) i Iptables  
/usr/portage/distfiles

najaktuelniju odgovarajuću verziju Iptables, npr. iptables-1.4.0.tar.bz2,  
otpakujte u

/paketi/Net/Sigurnost/Iptables-Netfilter/

cd /paketi/Net/Sigurnost/Iptables-Netfilter/

In -s ./iptables-1.4.0 ./iptables

Da biste mogli koristiti runme za patch-ovanje [GNU/Linux Kernel](#)-a i Iptables-a

In -s /paketi/Net/Sigurnost/Iptables-Netfilter/iptables /usr/src/iptables

Da biste mogli patchovati sa Tarpit napravite

mkdir paketi/Net/Sigurnost/Iptables-Netfilter/Tarpit-Updates

## Kernel patch-ovanje

U ovu fajlu možete stavljati Vaše dopune (patch-eve) [GNU/Linux Kernel](#) a. Koristite samo [Vanilla Kernel](#), jer patch-evi rade većinom dobro samo na Vanilla (generičkim [GNU/Linux Kernel](#)-ima).

/home/bin/kernel/iptables/kernel-patch

## Iptables patch-ovanje

Može se patch-ovati samo ako je [GNU/Linux Kernel](#) već patch-ovan i startan.

Znači sad morate ako to nije urađeno reći

Napravite novi [GNU/Linux Kernel](#) sa patch-o-matic-ng dodatcima sa

```
/home/bin/kernel-make
```

Startajte novi [GNU/Linux Kernel](#).

Iptables mora da podržave dodatke, možete staviti u

```
/etc/portage/package.use i /etc/paludis/use.conf
```

```
net-firewall/iptables extensions
```

Koristite ovu komandu da patch-ujete Iptables sa svim patch-o-matic-ng dodatcima koje ste izabrali već pre sa kernel-patch fajlom.

```
/home/bin/kernel/iptables/iptables-patch
```

Na jednoj konzoli startajte

```
/home/bin/kernel/iptables/iptables-patch
```

i potverdite sa d ali još ne pritiskajte return.

Onda na drugoj konzoli recite za reinstalaciju Iptables sa patch-o-matic-ng dodatcima

```
emerge -a iptables
```

I potverdite i u istom momentu na prvoj konzoli iptables-patch i uživajte...

Ovo patchovanje sa iptables-patch morate ponoviti kod svake nove verzije iptables.

Sad je [SSH protokol](#) još sigurniji...

Nažalost novi Iptables se ne može instalirati sa geoip patchom.

[SSH, Kernel, Iptables, patch-o-matic](#)

[Iptables se mora obnoviti pre bilo kakvog patch-ovanja](#)

[Kernel patch-ovanje](#)

[Iptables patch-ovanje](#)

[Na početak](#)

## **NFS protokol, Network File System**

<http://www.freebsd.org/doc/en/books/handbook/network-nfs.html>

[http://onlamp.com/pub/a/bsd/2002/02/14/Big\\_Scary\\_Daemons.html](http://onlamp.com/pub/a/bsd/2002/02/14/Big_Scary_Daemons.html)

<http://www.freebsddiary.org/nfs.php>

<http://www.debianhelp.co.uk/nfs.htm>

<http://www.debianadmin.com/network-file-system-nfs-server-and-client-configuration-in-debian.html>

<http://nfs.sourceforge.net/>

[http://www.linuxquestions.org/linux/answers/Networking/Easy\\_NFS](http://www.linuxquestions.org/linux/answers/Networking/Easy_NFS)

[http://lugons.org/Uputstva/Opste/Network\\_File\\_System/](http://lugons.org/Uputstva/Opste/Network_File_System/)

<https://wiki.archlinux.org/index.php/NFS>

<https://wiki.archlinux.org/index.php/NFSv4>

<http://www.troubleshooters.com/linux/nfs.htm>

[https://en.wikipedia.org/wiki/Network\\_File\\_System](https://en.wikipedia.org/wiki/Network_File_System)

[https://en.wikipedia.org/wiki/Open\\_Network\\_Computing\\_Remote\\_Procedure\\_Call](https://en.wikipedia.org/wiki/Open_Network_Computing_Remote_Procedure_Call)

## **NFS za BSD**

Za [BSD](#) ne trebate ništa skoro da instalirate dosta je već u [FreeBSD Base paketima](#).

NFSv4

## NFS Version 4 Protocol

man nfsv4

exports

Define remote mount points for [NFS](#) mount requests

man exports

mountd

Service remote [NFS](#) mount requests

man mountd

showmount

Show remote [NFS](#) mounts on host

man showmount

nfsd

Remote [NFS](#) server

man nfsd

nfsuserd

Load user and group information into the kernel for [NFSv4](#) services

man nfsuserd

nfsstat

Display [NFS](#) statistics

```
man nfsstat
```

nfsiod

Local [NFS](#) asynchronous I/O server

```
man nfsiod
```

nfscbd

[NFSv4](#) client side callback daemon

```
man nfscbd
```

rpcbind

Universal addresses to RPC program number mapper

```
man rpcbind
```

rpcinfo

Report RPC information

```
man rpcinfo
```

Pogledajte koje su normalne vrednosti za [NFS](#) podešavanja za [/etc/rc.conf](#)

```
grep nfs /etc/defaults/rc.conf
```

*Kraj NFS za BSD*

[\*\*NFS za Debian GNU/Linux\*\*](#)

Za klijenta

```
apt-get install nfs-common portmap
```

Za servera

```
apt-get install nfs-kernel-server nfs-common portmap
```

*Kraj NFS za Debian GNU/Linux*

## **NFS za Gentoo**

Morate imati podešen [Kernel](#) da bi Vam radio [NFS](#).

### **NFS client and server daemons**

<http://linux-nfs.org>

```
emerge -a nfs-utils
```

## **NFSv4**

NFSv4 ID <-> name mapping library

<http://www.citi.umich.edu/projects/nfsv4/linux/>

```
emerge -a libnfsidmap
```

Podesite Vaše [Hostname](#) koje koristite na serveru isto za klijent u

/etc/idmapd.conf

```
Domain = hostname
```

Ako to ne podesite pravilno onda pripada korisniku nobody, grupa nobody

## **Netkit - portmapper**

Sa novim verzijama [nfs-utils](#) više nije potrebno.

<http://ftp.porcupine.org/pub/security/index.html>

emerge -a portmap

*Kraj NFS za Gentoo*

## **Primer za NFS klijenta**

<http://en.gentoo-wiki.com/wiki/NFS/Client>

Obavezno dobro proučite

man mount\_nfs

Potrebno je da podesite

</etc/fstab>

```
# Network File System, only for Client, man mount_nfs
192.168.2.3:/zajedno1 /zajedno1 nfs rw,noatime,bg,hard,tcp 0 0
192.168.2.3:/zajedno2 /zajedno2 nfs rw,noatime,bg,hard,tcp 0 0
```

Da mountujete sa NFS Server-a, na primer, naravno ako je </etc/fstab> podešen

mount 192.168.2.3:/usr/ports/distfiles /usr/ports/distfiles

mount 192.168.2.3:/paketi /paketi

Podignite ga sa

Za BSD

```
/etc/rc.d/nfsclient onestart
```

Za [GNU/Linux](#)

```
/etc/init.d/nfsmount start
```

Da se uvek starta pri podizanju sistema

Za [BSD](#)

```
/etc/rc.conf
```

```
# Network File System

# For NFS Server and Client
rpcbind_enable="YES"
nfsuserd_enable="YES"

# For NFS Server
#mountd_enable="YES"
#mountd_flags="-r -p NFS-Port"
##mountd_flags="-r"
#nfs_server_enable="YES"
#nfsv4_server_enable="YES"
#rpc_lockd_enable="YES"
#rpc_stattd_enable="YES"

# For NFS Client
nfs_client_enable="YES"
nfscbd_enable="YES"

# End Network File System
```

Za [GNU/Linux](#)

```
rc-update add nfsmount default
```

Da restartujete

Za [BSD](#)

```
/etc/rc.d/nfsclient restart
```

Za [GNU/Linux](#)

```
/etc/init.d/nfsmount restart
```

## Primer za [NFS Server](#)

<http://en.gentoo-wiki.com/wiki/NFS/Server>

Podignite ga sa

Za [BSD](#)

```
/etc/rc.d/nfsd onestart
```

```
/etc/rc.d/nfsuserd onestart
```

Za [GNU/Linux](#)

```
/etc/init.d/nfs start
```

Da se uvek starta pri podizanju sistema

Za [BSD](#)

[/etc/rc.conf](#)

```
# Network File System

# For NFS Server and Client
rpcbind_enable="YES"
nfsuserd_enable="YES"

# For NFS Server
mountd_enable="YES"
mountd_flags="-r -p NFS-Port"
#mountd_flags="-r"
nfs_server_enable="YES"
nfsv4_server_enable="YES"
rpc_lockd_enable="YES"
rpc_statd_enable="YES"
```

```
# For NFS Client  
#nfs_client_enable="YES"  
#nfscbd_enable="YES"  
  
# End Network File System
```

Za [GNU/Linux](#)

```
rc-update add nfs default
```

Potrebno samo za Server, podešavate šta izvozite

```
/etc(exports
```

Ako nemate tu fajlu napravite je sa

```
touch /etc(exports
```

Primer koji radi, korisnik [root](#) i posebna grupa u kojoj su [normalni korisnik](#) i [korisnik za igre i emulatore](#)

```
/etc(exports
```

```
/zajedno1 -maproot=0:XY00 -network 192.168.2.0/24  
/zajedno2 -maproot=0:XY00 -network 192.168.2.0/24
```

Ne treba podešavati [/etc/fstab](#), samo klijent to mora da podešava.

Da exportujete /etc/exports to jest da se ponovo učita

Za [BSD](#)

```
/etc/rc.d/mountd onereload
```

Za [GNU/Linux](#)

```
exportfs -ra
```

Da vidite šta eksportujete

```
exportfs -v
```

Pogledajte da nemate neke greške pri exportovanju /etc/export u  
/var/log/messages

Da vidite na drugi način šta eksportujete, morate tako pisati direktorijume u [/etc/fstab](#) kod klijenta

```
showmount --help
```

```
showmount -e
```

Exports list on localhost:  
/zajedno2 192.168.2.0  
/zajedno1 192.168.2.0

Da vidite šta ste sve eksportovali

```
showmount -a
```

## Sigurnost za NFS

NFS protokol je normalno veoma nesiguran.

<http://tldp.org/HOWTO/NFS-HOWTO/security.html>

<http://biowiki.org/MountingNFSThroughSSHTunnel>

<http://wiki.debian.org/SecuringNFS>

<https://code.google.com/p/macnfsv4/wiki/FreeBSD8KerberizedNFSSetup>

Možete koristiti [NFS](#) sa [Stunnel](#)

[https://w3.physics.illinois.edu/physwiki/doku.php?id=pcs:unix:nfs\\_over\\_stunnel](https://w3.physics.illinois.edu/physwiki/doku.php?id=pcs:unix:nfs_over_stunnel)

## Ako imate probleme sa [NFS](#)-om

Morate dopustiti Vašim klijentima da bi mogli mountovati neke direktorijume

/etc/hosts.allow

/etc/hosts.deny

<http://www.freebsddiary.org/nfs-portmap.php>

<http://www.freebsddiary.org/nfs.php>

Da vidite da li radi mreža

sockstat -4

ps -ax | grep rpc

Kontrola na serveru

netstat -a -n | grep 2049

rpcinfo -p | egrep 'nfs|nlock'

Kontrola na klijentu

grep nfs /etc/fstab

rpcinfo -p host

rpcinfo -p | grep nlock

```
netstat -a -n | grep 2049
```

```
rpcinfo -u hostname nfs
```

```
rpcinfo -u hostname mountd
```

```
rpcinfo -t hostname nfs
```

```
rpcinfo -t hostname mountd
```

Na serveru prekinite ovim redom pri problemima

**nfsd -> mountd -> rpcbind**

Na serveru podignite ovim redom pri problemima

**rpcbind -> mountd -> nfsd**

Za [BSD](#)

```
/etc/rc.d/nfsd stop
```

```
/etc/rc.d/mountd stop
```

```
/etc/rc.d/rpcbind stop
```

```
/etc/rc.d/rpcbind start
```

```
/etc/rc.d/mountd start
```

```
/etc/rc.d/nfsd start
```

Za [GNU/Linux](#)

```
/etc/init.d/nfs stop
```

```
/etc/init.d/mountd stop
```

```
/etc/init.d/rpcbind stop
```

```
/etc/init.d/rpcbind start
```

```
/etc/init.d/mountd start
```

```
/etc/init.d/nfs start
```

Da vidite razne informacije

```
rpcinfo
```

Koji se Portovi koriste

```
rpcinfo -p
```

```
rpcinfo -p localhost
```

I za servera i za klijenta stavite Vaše kompjutere da se vide u

```
/etc/hosts
```

Da vidite šta je mountovano sa servera

```
df -h | grep 192.168
```

[NFS protokol, Network File System](#)

[Primer za NFS klijenta](#)

[Primer za NFS Server](#)

[Sigurnost za NFS](#)

[Ako imate probleme sa NFS-om](#)

[Na početak](#)

## **Upotreba Rsync-a**

Veoma koristan je [Rsync](#) za osiguravanja na više kompjutera.

Da li imate sve potrebne [USE](#)?

Ne morate obavezno da koristite daemon za [Rsync](#).

Obavezno pogledajte

**man rsync**

**man rsyncd.conf**

isto što i

<http://rsync.samba.org/ftp/rsync/rsync.html>

<http://rsync.samba.org/ftp/rsync/rsyncd.conf.html>

<http://samba.anu.edu.au/rsync/documentation.html>

Kanal #rsync na [Freenode](#)

<http://sanitarium.net/rsyncfaq/>

Developer Kevin Korb, nick BasketCase

<http://www.visionquest.net/Video.php>

<http://www.sanitarium.net/>

[http://sanitarium.net/unix\\_stuff/rspaghetti\\_backup/readme.txt](http://sanitarium.net/unix_stuff/rspaghetti_backup/readme.txt)

[http://www.sysresccd.org/Sysresccd-manual-en\\_Backup\\_and\\_transfer\\_your\\_data\\_using\\_rsync](http://www.sysresccd.org/Sysresccd-manual-en_Backup_and_transfer_your_data_using_rsync)

[http://www.ibm.com/developerworks/aix/library/au-spunix\\_rsync/index.html](http://www.ibm.com/developerworks/aix/library/au-spunix_rsync/index.html)

[http://www.mikerubel.org/computers/rsync\\_snapshots/](http://www.mikerubel.org/computers/rsync_snapshots/)

<http://www.linuxjournal.com/article/6475>

<http://www.linuxjournal.com/article/6508>

<http://www.linux.com/archive/articles/113847>

<https://wiki.archlinux.org/index.php/Rsync>

**Možete koristiti [root](#) nalog za [OpenSSH](#) samo za restriktivni [Rsync](#)**

Naravno možete koristiti i [korisnika za delenje](#) samo za restriktivni [Rsync](#).

Pogledajte [SSH protokol](#), posebno odeljak [Možete koristiti root nalog za OpenSSH](#)

Kako da radi sigurno [OpenSSH](#) sa [Rsync](#), a da imate prava [administratora](#)

<http://www.sanitarium.net/rsyncfaq/#sudo>

[http://linsec.ca/Optimizing\\_OpenSSH](http://linsec.ca/Optimizing_OpenSSH)

[Rsync](#) skripte

<http://www.samba.org/ftp/unpacked/rsync/support/>

Restricts [Rsync](#) skripta

<http://www.samba.org/ftp/unpacked/rsync/support/rrsync>

Starija verzija

<http://www.inwap.com/mybin/miscunix/?rrsync>

Da bi mogli koristili maksimalnu zaštitu za [Rsync](#), restriktivni [Rsync](#), treba da linkujete ovu skriptu sa

Za [BSD](#)

Možete skinuti sa Interneta ili kopirati iz [GNU/Linux-a](#) i otpakovati

**mkdir -p /paketi/Net/Rsync/support**

**In -s /paketi/Net/Rsync/support/rrsync /usr/local/bin/rrsync**

Za [GNU/Linux](#)

**In -s /usr/share/rsync/rrsync /usr/local/bin/rrsync**

Pazite default neće da kopira ako je na kompjuteru na koji se kopira ta fajla novija.

Pogledajte ove skripte koje veoma olakšavaju rad sa [Rsync](#)-om, sve skoro radi automatski.

Ova skripta se zove od ostalih rsync-\* skripti za osiguravanje i starta Vaš [PDF preglednik](#) sa logom koji je napravljen pri osiguravanju sa [Rsync](#)-om

```
/home/bin/rsync-report-pdf
```

Možete imati logove prema Hostovima (kompjuterima na koje osiguravate) i prema skriptama sa kojima osiguravate (što znači po direktorijumima).

```
/home/bin/rsync-*
```

Podesite ih prema Vašim potrebama, ne koristite ih dok ne proverite da li rade kod Vas, šta rade i uvek prvo dodajte opciju **--dry-run** da vidite šta se događa.

```
RSYNC="rsync ... --dry-run"
```

Probajte uvek prvo da vidite šta će da bude

```
rsync ... --dry-run
```

Da vidite šta će tačno da se desi, i razlog zbog čega se nešto isključuje

```
rsync ... --dry-run -v -v
```

Preporučujem da napravite direktorijum gde će se čuvati Vaši logovi na primer

```
mkdir -p /var/log/MyLog/
```

Možete koristiti [Rsync](#) sa [Stunnel](#), mada je bolje sa [SSH Tunnel](#)-om

[http://www.netbits.us/docs/stunnel\\_rsync.html](http://www.netbits.us/docs/stunnel_rsync.html)

Da vidite šta je podignuto za [Rsync](#)

```
ps auxw | grep rsync
```

Možete proveriti da li imate [SSH Tunnel](#) i da li se koristi na primer sa

```
netstat -an | grep IP-adresa
```

Da vidite koje IP adrese sluša Vaš-port za [Rsync](#)

```
netstat -an | grep Vaš-port
```

```
tcp      0      0 127.0.0.1:Vaš-port      0.0.0.0:*          LISTEN
```

Ako dobijete na primer ovu grešku, to znači da nemate čistu konfiguraciju za Vaš [Shell](#), nešto smeta u konfiguracionim fajlama, nađite šta je to i nećete imati više ovu grešku

```
protocol version mismatch - is your shell clean?
```

<http://www.hostanswers.net/linux-hosting/rsync-protocol-version-mismatch/>

Meni ovi programi nisu potrebni, jer sve što mi treba mogu da uradim sa skriptama.

## Grsync

A Gtk frontend to [Rsync](#)

Najbolje da ga koristi korisnik koji može da se uloguje.

<http://www.opbyte.it/grsync/>

Za [BSD](#)

```
portmaster -n net/grsync
```

Za [GNU/Linux](#)

```
emerge -a grsync
```

## rdiff-backup

Remote incremental file backup utility;  
uses librsync's rdiff utility to create concise, versioned backups

<http://www.nongnu.org/rdiff-backup/>

Za BSD

```
portmaster -n sysutils/rdiff-backup
```

Za GNU/Linux

```
emerge -a app-backup/rdiff-backup
```

```
man rdiff-backup
```

## **Lsyncd**

Live Syncing (Mirror) Daemon

[https://code.google.com/p/lSyncd/](https://code.google.com/p/lsyncd/)

```
emerge -a lsyncd
```

```
man lsyncd
```

```
lsyncd -help
```

Na početak

## **NAS, Network-Attached Storage**

[https://en.wikipedia.org/wiki/Network-attached\\_storage](https://en.wikipedia.org/wiki/Network-attached_storage)

<http://www.nasstorageserver.com/>

Kako se nastao OpenMediaVault od FreeNAS.

<http://blog.freenas.org/2009/12/freenas-ready-for-next-step.html>

<http://www.learnfreenas.com/blog/2009/12/05/rumours-of-freenas-death-greatly->

exaggerated/

## FreeNAS

Is a free, open source, Network-Attached Storage operating system based on FreeBSD.

<http://www.freenas.org/>

<https://en.wikipedia.org/wiki/Freenas>

Koristi kod od m0n0wall kao i pfSense.

FreeNAS nije potpuno Free Software kao FreeBSD.

FreeNAS pripada i podržan je od iXsystems.

TrueNAS™

Is a Network-Attached Storage operating system based on the FreeBSD operating system.

<http://www.ixsystems.com/ix/support/software/truenas-support>

<http://www.ixsystems.com/ix/storage/titan-truenas-pro>

FreeNAS dokumentacija

[http://doc.freenas.org/index.php/Main\\_Page](http://doc.freenas.org/index.php/Main_Page)

[http://doc.freenas.org/index.php/Installing\\_FreeNAS](http://doc.freenas.org/index.php/Installing_FreeNAS)

FreeNAS forum

<http://forums.freenas.org/>

Kanal #freenas na Freenode

<http://www.learnfreenas.com/blog/>

FreeNAS 8 Tips, Tricks, and Tutorials

<http://protosd.blogspot.com/>

Kako da radi FreeBSD Jails sa FreeNAS, ima više sličnih primera

<http://protosd.blogspot.com/2011/12/howto-install-jdownloader-in-freebsd.html>

<http://forums.freenas.org/showthread.php?2672-HOWTO-Install-JDownloader-in-a-FreeBSD-Jail>

Idiot's guide to installing [FreeNAS](#)

<http://blog.patyen.com/lessons/technology/idiot%E2%80%99s-guide-to-installing-freenas/>

Možete za [FreeNAS](#) promeniti IP adresu na primer sa

```
ifconfig em0 192.168.2.13 netmask 255.255.255.0
```

```
route add default 192.168.2.101
```

Možete koristiti [FreeNAS](#) u [emulatorima za operativne sisteme](#)

[http://doc.freenas.org/index.php/Installing\\_FreeNAS](http://doc.freenas.org/index.php/Installing_FreeNAS)

<http://www.freebsdnews.net/2009/03/06/freenas-virtualbox-installation/>

## **OpenMediaVault**

Is the next generation network attached storage (NAS) solution based on [Debian GNU/Linux](#). It contains services like SSH, (S)FTP, SMB/CIFS, DAAP media server, RSync, BitTorrent client and many more. Thanks to the modular design of the framework it can be enhanced via plugins.

<http://openmediavault.org/>

<https://en.wikipedia.org/wiki/OpenMediaVault>

[Na početak](#)

## **SSL protokol**

### **OpenSSL**

Osnova za SSL protokol

<http://www.openssl.org>

Za [BSD](#)

[OpenSSL](#) se nalazi u [FreeBSD Base paketima](#).

Ako hoćete da koristite u BSD-u noviji OpenSSL, pazite može da ne rade onda mnogi FreeBSD Ports

```
portmaster -n security/openssl
```

Koristite samo OpenSSL kao opciju u svim FreeBSD Ports a GNUTLS svuda isključite.

Za GNU/Linux

```
emerge -a openssl
```

Kako da napravite ručno certifikate

<http://www.vompatti.fi/~vesse/texts/openssl/>

<http://www-user.tu-chemnitz.de/~hot/SSL/>

<http://www.onsight.com/faq/stunnel/stunnel-faq-a.html>

[http://linuxnet.ch/groups/linuxnet/wiki/01946/HOWTO\\_Create\\_SSL\\_Certificate.html](http://linuxnet.ch/groups/linuxnet/wiki/01946/HOWTO_Create_SSL_Certificate.html)

[http://linuxnet.ch/groups/linuxnet/wiki/5ee79/Working\\_with\\_OpenSSL\\_Certificates.html](http://linuxnet.ch/groups/linuxnet/wiki/5ee79/Working_with_OpenSSL_Certificates.html)

<http://www.tldp.org/HOWTO/SSL-Certificates-HOWTO/>

<http://sandbox.rulemaker.net/ngps/m2/howto.ca.html>

<http://www.madboa.com/geek/openssl/>

<http://www.debian-administration.org/articles/284>

<http://www.zimbio.com/Linux/articles/UXP0ymrxfUI/Apache+SSL+Certificate+Authority+CA+Howto>

<http://sandbox.rulemaker.net/ngps/m2/howto.ca.html>

<http://www.slingcode.com/pki.php>

<http://lists.freebsd.org/pipermail/freebsd-security/2011-April/thread.html>

```
/home/bin/openssl-server
```

Pogledajte Stunnel skripte, dobri primeri kako da pravite Vaše certifikate.

Da proverite Vaš certifikat

```
openssl x509 -subject -dates -fingerprint -in Vaš.pem
```

Da povučete neki certifikat

```
openssl ca -revoke newcert.pem
```

Da obnovite Vašu bazu za [SSL](#)

```
openssl ca -updatedb
```

```
openssl version -d
```

```
OPENSSLDIR: "/etc/ssl"
```

## NSS, Network Security Services

Is a set of libraries designed to support cross-platform development of security-enabled server applications. Applications built with NSS can support SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 certificates, and other security standards.

<http://www.mozilla.org/projects/security/pki/nss/>

Za [BSD](#)

```
portmaster -n security/nss
```

Za [GNU/Linux](#)

```
emerge -a dev-libs/nss
```

Možete imati [NSS](#) u pem formatu

<http://curl.haxx.se/docs/caextract.html>

## Common CA Certificates

Root certificates from certificate authorities included in the Mozilla [NSS](#) library and thus in Firefox and Thunderbird.

Trebate imati i certifikate, da bi se mogli identifikovati

<http://packages.debian.org/sid/ca-certificates>

Za [BSD](#)

```
portmaster -n security/ca_root_nss
```

Za [GNU/Linux](#)

```
emerge -a ca-certificates
```

Može se desiti da imate loše linkove, to možete ovako rešiti

```
find -L /etc/ssl/certs/ -type l -exec rm {} +
```

U svakom slučaju treba da bude fajla, koja može da se čita od Vaših korisnika

```
/usr/local/share/certs/ca-root-nss.crt
```

Ako Vaši korisnici nemaju prava da čitaju [Common CA Certificates](#) to znači da ne mogu da ih koriste

```
ls -lh /usr/local/share/certs
```

```
ls: /usr/local/share/certs: Permission denied
```

Zato promenite prava kao [root](#)

```
chmod 750 /usr/local/share/certs
```

Proverite kao korisnik

```
ls -lh /usr/local/share/certs
```

```
-r--r--r-- 1 root wheel 723k datum ca-root-nss.crt  
-rw-r--r-- 1 root wheel 2.8k datum spicacert.crt
```

Ako dobijete probleme kao, probajte jednostavno da izbrišite sve nss pakete i novo instalšite

```
Connection failed. Error: unable to get local issuer certificate.? (20)
```

```
Connection failed. Error: certificate not trusted.? (27)
```

Probajte da se konektujete sa

```
openssl s_client -connect hostname:port
```

```
openssl s_client -connect mail.gmx.net:465
```

```
openssl s_client -connect sourcecoast.com:443
```

```
openssl s_client -connect www.thawte.com -port 443
```

Treba da vidite, ako je sve u redu

```
Verify return code: 0 (ok)
```

Ako imate greške dobićete verovatno

```
Verify return code: 20 (unable to get local issuer certificate)
```

Probajte da kopirate od -----BEGIN CERTIFICATE----- do -----END CERTIFICATE----- u novu fajlu

/usr/local/share/certs/mail.gmx.net.pem

```
openssl s_client -CAfile mail.gmx.net.pem -connect mail.gmx.net:465
```

Verify return code: 0 (ok)

## create-cert

Is a script that uses [OpenSSL](#) to create self-signed host certificates and private keys for fully qualified domain names (FQDNs).

Za [BSD](#)

```
portmaster -n security/create-cert
```

```
man create-cert
```

Pravi konfiguracionu fajlu /root/create-cert.conf

```
cd
```

```
create-cert -l
```

```
create-cert -R
```

## TinyCA

Simple Perl/Tk [GUI](#) to manage a small certification authority

[GUI](#) za pravljenje SSL ključeva, Certifikata, sve to može i ručno.

<http://tinyca.sm-zone.net>

[http://www.linux-magazin.de/online\\_artikel/schluesseldienst?category=0](http://www.linux-magazin.de/online_artikel/schluesseldienst?category=0)

Za [BSD](#)

```
portmaster -n security/tinyca
```

Za [GNU/Linux](#)

```
emerge -a app-crypt/tinyca
```

## Ručno podešavanje OpenSSL-a.

Podesiti prema primeru iz mojih fajli ili na neki drugi način.

```
cd /etc/ssl
```

Upišite Vaše podatke u openssl.cnf da ih ne bi morali stalno unositi pri pravljenju Certifikata.

Pre pravljenja ključeva uradite

```
mkdir demoCA && echo 01 > demoCA/serial
```

da ne dobijete grešku

```
No such file or directory:bss_file.c:398:fopen('./demoCA/serial','r')
```

## /etc/ssl/openssl.cnf

Stavite na dva mesta na optional da ne dobijete grešku

```
The commonName field needed to be supplied and was missing
```

```
# For the CA policy i za # For the 'anything' policy
```

```
commonName<----><----->= optional
```

Da ne bi dobijali ove greške, ako imate više Certifikata

failed to update database  
TXT\_DB error number 2

Možete i ovo probati da obnovite Databasu

openssl ca -updatedb

[ CA\_default ]

unique\_subject = no

Pišite Vaše podatke samo u ovom odeljku

[ req\_distinguished\_name ]

...  
Državu

Provinciju

Mesto

Kompaniju, samo da nešto piše

Email adresu, ne pišite pravu ako je samo za privatno

[SSL protokol](#)  
[OpenSSL](#)  
[Common CA Certificates](#)  
[create-cert](#)  
[TinyCA](#)  
[Ručno podešavanje OpenSSL-a](#)  
[Na početak](#)

## **FTP protokol, File Transfer Protokol**

<http://slacksite.com/other/ftp.html>

<https://secure.wikimedia.org/wikipedia/en/wiki/Ftp>

<http://mimar.rs/za-stvaraoce/ftp-server-sa-virtualnim-korisnicima/>

Šta sve postoji

Za [BSD](#)

```
cd /usr/ports/ftp ; ls
```

Za [GNU/Linux](#)

```
eix ftp
```

```
eix -S ftp
```

## **[vsftpd, Very Secure FTP Deamon](#)**

Very Secure FTP Daemon written with speed, size and security in mind

Ovo je veoma siguran FTP Server

<http://vsftpd.beasts.org>

<http://viki.brainsware.org/>

Kanal #vsftpd na [Freenode](#)

Za [BSD](#)

Postoji [PBI](#) paket.

```
portmaster -n ftp/vsftpd
```

Za [GNU/Linux](#)

```
emerge -a vsftpd
```

## **Podešavanja za [vsftpd, Very Secure FTP Deamon](#)**

<http://rimuhosting.com/howto/ftp.jsp>

<http://wjholden.com/vsftpd-help.html>

Za BSD

```
cd /usr/local/etc/
```

Za GNU/Linux

```
cd /etc/vsftpd
```

Podesite vsftpd konfiguraciju

Za BSD

```
/usr/local/etc/vsftpd.conf
```

Za GNU/Linux

```
/etc/vsftpd/vsftpd.conf
```

Možete napraviti sa ovom skriptom Vaš OpenSSL vsftpd ključ

```
/home/bin/openssl-vsftpd-server
```

Da podignite server

Za BSD

```
/usr/local/etc/rc.d/vsftpd onestart
```

Za GNU/Linux

```
/etc/init.d/vsftpd start
```

Da se uvek starta pri podizanju sistema

Za BSD

```
/etc/rc.conf
```

```
vsftpd_enable="YES"
```

Za [GNU/Linux](#)

```
rc-update add vsftpd default
```

Primer

```
/etc/hosts.allow
```

## LFTP

A sophisticated ftp/sftp/http/https/torrent client and file transfer program

[Konzolni](#) FTP program, on radi uvek

<http://lftp.yar.ru/>

Za [BSD](#)

Postoji [PBI](#) paket.

```
portmaster -n ftp/lftp
```

Za [GNU/Linux](#)

```
emerge -a lftp
```

## gFTP

GTK FTP klijent

<http://www.gftp.org/>

Za [BSD](#)

Postoji [PBI](#) paket.

```
portmaster -n ftp/gftp
```

Za [GNU/Linux](#)

```
emerge -a gftp
```

## KFTPgrabber

FTP client for K Desktop Environment

[KDE](#) FTP klijent, podržava SSL

<http://kftpgrabber.sourceforge.net>

Za [BSD](#)

```
portmaster -n ftp/kftpgrabber
```

Za [GNU/Linux](#)

Ne postoji više u [Gentoo](#)-u

```
emerge -a kftpgrabber
```

## FileZilla

FTP client with lots of useful features and an intuitive interface

Postoji i za [smopu!M](#), za mene malo previše

<http://filezilla-project.org>

Za [BSD](#)

Postoji [PBI](#) paket.

```
portmaster -n ftp/filezilla
```

Za [GNU/Linux](#)

```
emerge -a filezilla
```

[FTP protokol, File Transfer Protokol](#)  
[vsftpd, Very Secure FTP Deamon](#)  
[Podešavanja za Very Secure FTP Deamon](#)  
[LFTP](#)  
[gFTP](#)  
[KFTPgrabber](#)  
[FileZilla](#)  
[Na početak](#)

## **Layer 5**

Deep Web

<http://deep-web.org/>

<http://deep-web.org/how-to-research/deep-web-search-engines/>

<http://maddsgn.weebly.com/1/post/2012/09/deep-web.html>

[http://www.tcpipguide.com/free/t\\_SessionLayerLayer5.htm](http://www.tcpipguide.com/free/t_SessionLayerLayer5.htm)

<http://thehackernews.com/2012/05/what-is-deep-web-first-trip-into-abyss.html>

[https://en.wikipedia.org/wiki/Deep\\_Web](https://en.wikipedia.org/wiki/Deep_Web)

<http://www.youtube.com/watch?v=SII38b0RJr8>

[Na početak](#)

## **Radius protokol, Remote Authentication Dial In User Service**

<http://en.wikipedia.org/wiki/RADIUS>

[http://en.wikipedia.org/wiki/List\\_of\\_RADIUS\\_servers](http://en.wikipedia.org/wiki/List_of_RADIUS_servers)

## **GNU Radius**

GNU radius authentication server

<http://www.gnu.org/software/radius/radius.html>

emerge -a gnuradius

## FreeRADIUS

Highly configurable free RADIUS server

<http://freeradius.org/>

emerge -a freeradius

## FreeRADIUS Client

FreeRADIUS Client framework

<http://wiki.freeradius.org/Radiusclient>

emerge -a freeradius-client

[Radius protokol, Remote Authentication Dial In User Service](#)  
[Na početak](#)

## VPN protokol, Virtual Private Network

Ovo je veoma dobar protokol za tunel između kompjutera.

Bolje je da imate [Router](#) i da njega koristite za [VPN protokol](#).

Da vidite šta sve postoji

eix -S vpn

## OpenVPN

A robust and highly flexible tunneling application compatible with many OSes

Radi kao Daemon, User Space, slično kao [OpenSSH](#)

<http://openvpn.net>

emerge -a openvpn

Obavezno ovo pročitajte, odlična objašnjenja

<http://openvpn.net/faq.html>

<http://wiki.openwrt.org/oldwiki/openvpntunhowto>

Koristite na obe strane samo tun (Routing) ili tap (Brining). Preporučujem tun.

Veoma dobra objašnjenja i odličan PDF

<http://www.buildinglinuxvpns.net/>

Odličan forum i Wiki, nemački

<http://forum.openvpn.eu/>

<http://wiki.openvpn.eu/index.php/Hauptseite>

Malo starije, ali ima dobra objašnjenja

<http://openvpn.net/papers/BLUG-talk/index.html>

Perfect Privacy ima odlična objašnjenja

<https://forum.perfect-privacy.com/showthread.php?t=1019>

<https://forum.perfect-privacy.com/showthread.php?t=1013>

Performance Analysis of OpenVPN on a Consumer Grade Router

<http://www.cse.wustl.edu/~jain/cse567-08/ftp/ovpn/index.html>

OpenWPN i DD-WRT na Linksys Routeru

<http://blog.zenone.org/2008/01/openvpn-and-dd-wrt-on-linksys-wrt54gl.html>

Dobar pdf

<http://www.leinonen.org/pfsense.html>

```
mkdir -p /paket/Net/Sigurnost/OpenVPN  
cd /paket/Net/Sigurnost/OpenVPN
```

```
wget / http://leinonen.org/Softat/How_to_configure_OpenVPN_shared_key_tunnels_using_pf-  
Sense_and_OpenWRT.pdf
```

## **Pravljenje ključeva, Certifikata i potpisivanje**

Pogledajte šta da radite dok pravite ključeve.

Ovde imate odlična objašnjenja kako i zašto se prave ključevi, njihova razmena, postupak da sve proradi i konfiguracije Server-a i Client-a. Preporučujem jer je stvarno odlilčno.

<http://www.lagged.za.net/mediawiki/index.php/OpenVPN>

## **CA, Certificate Authority postupak**

**Ovo se radi na Server-u!**

**To mora biti siguran komjuter, koji je samo pod Vašom kontrolom.**

**Gde ne može tako lako neki Hacker da uđe i da zloupotrebi  
Vaše privatne ključeve i da sa njima potpiše svoje Certifikate  
i tako dobije pristup na kompjutere koje Vi održavate ili koristite!**

Napravite Vaše lične ključeve, bolje nego statični ključevi koji su opšte poznati.

Preporučujem da OpenVPN Certifikate i ključeve ne mešate sa OpenSSL Certifikatima od drugih programa.

Na kraju ovog odeljka imate fajlu koja sve ove korake radi automatski za Server.

```
/home/bin/openssl-openvpn-server
```

Napravite direktorijum za Vaš CA, ne mešajte ove ključeve i Certifikate sa Vašim ključevima i Certifikatima za upotrebu OpenVPN.

Ovo je samo za pravljenje ključeva, Certifikata i njihova potpisivanja.

```
mkdir /etc/openvpn/CA
```

Uđite u direktorijum

```
cd /etc/openvpn/CA
```

Napravite direktorijume

```
mkdir certs newcerts private
```

Komande su veoma duge, zato sam ih razdvojio sa "\" da su u dva ili više redova, mada su samo jedan red.

### **Pravljenje CA key, koristite najjaču zaštitu od 4096 bita**

```
openssl genrsa -aes256 -out private/openvpn-cakey.pem 4096
```

### **Pravljenje CA Certifikata**

```
openssl req -new -newkey rsa:4096 -x509 -days 3650 -key private/openvpn-cakey.pem \  
-out openvpn-ca.pem
```

Dobra je ideja da se sada napravi index.txt

```
touch index.txt
```

Takođe da se napravi i serial fajla za brojanje Certifikata

```
echo 01 > serial
```

## Pravljenje CSR, Certificate Signing Request

Da bi se mogao napraviti par ključeva za Servera i Klijenta

Koristiti "-nodes" da se pri svakom startanju Servera ne mora pisati šifra.

```
openssl req -new -newkey rsa:4096 -out certs/openvpn-server-csr.pem \
-nodes -keyout private/openvpn-server-key.pem -days 99999
```

## Pravljenje Certifikata za Server

```
openssl x509 -req -in certs/openvpn-server-csr.pem -out certs/openvpn-server-cert.pem \
-CA openvpn-ca.pem -CAkey private/openvpn-cakey.pem -days 3650
```

## OpenVPN Daemon CA Files

<http://openvpn.net/index.php/documentation/howto.html>

Pogledajte pod **Key Files**

ca.crt Server + all Clients, Root CA certificate, No Secret

**CA javni ključ.** Potvrđuje OpenVPN da je openvpn-server-cert.pem potpisana sa CA ključem.

Ova CA informacija je javna i treba da bude na svim kompjuterima u OpenVPN mreži.

/etc/openvpn/CA/openvpn-ca.pem

ca.key, Key signing Machine only, Root CA key, Yes Secret

**Tajni ključ CA.** Smi biti samo na kompjuteru koji pravi Certifikate.

/etc/openvpn/CA/private/openvpn-cakey.pem

dh{n}.pem, Server only, Diffie Hellman parameters

/etc/openvpn/keys/dh2048.pem

server.crt, Server only, Server Certificate, No Secret

Je potpisani Certifikat, pravi plus openvpn-ca.pem sumu za proveravanje (checksum) koja proverava protiv privatnog ključa, dobra je ideja da se ova fajla čuva od svih pogleda iako nije suviše važna. Samo na Server-u.

/etc/openvpn/CA/certs/openvpn-server-cert.pem

Server.key, Server only, Server Key, Yes Secret

**Tajni ključ Servera.** Pravi plus openvpn-ca.pem sumu za proveravanje (checksum) koja proverava protiv openvpn-server-cert.pem da garantuje autentičnost, to je tajna fajla i ona sme da se čita samo od OpenVPN CA i nikoga više. Samo na Server-u.

/etc/openvpn/CA/private/openvpn-server-key.pem

client1.crt, Client1 only, Client1 Certificate, No Secret

Certifikat Klijenta. Samo kod klijenta.

openvpn-klijent-cert.pem

client1.key, Client1 only, Client1 Key, Yes Secret

**Tajni ključ Klijenta.** Samo kod klijenta.

openvpn-klijent-key.pem

TLS key, this is used in handshaking

If a tls-auth key is used on the server

then every client must also have the key

**Je tajni sigurnosni ključ. Svuda u OpenVPN mreži.**

ta.key

Originalni zahtev za potpis Certifikata, može se posle potpisa obrisati

openvpn-klijent-csr.pem

## OpenVPN Certificate Management

Vaš klijent želi da napravi zahtev za Certifikat od poverljive strane (to je Vaš OpenVPN CA) i želi da CA potpiše i tako potvrdi da je validan korisnik od OpenVPN-a.

### Zahtev klijenta za potpis Certifikata

To mora da uradi Klijent!

Napravio sam ovu fajlu za pravljenje Certifikata koji treba da se potpišu.

Takođe podešava prava fajli i direktorijuma, pakuje Certifikat i briše ga, jer on treba samo Serveru za potpis.

Dajte samo ime klijenta i eventualno promenite koliko dana da bude validan Vaš Certifikat.

Trebate da imate instalisan openSSL.

Kod klijenta ne treba koristiti "-nodes", da bi bili sigurni da se niko ne može priključiti na Server bez šifre. Na primer ako nestane Laptop sa potpisanim Certifikatom.

```
/home/bin/openssl-openvpn-klijent
```

Pošaljite Vaš paket Vašem CA Server-u preko sigurne [SSH](#) veze na potpis.

### **Potpisivanje Certifikata klijenta pomoću CA**

To mora da uradi Server!

Primili ste openvpn-klijent-csr.pem za potpis od Klijenta,  
prebacite ga u /etc/openvpn/newcerts/

Napravio sam ovu fajlu za potpisivanje Certifikata klijentima.

Ona potpisuje, pravi paket, briše nepotrebne fajle, koje više ne trebaju na Server-u.

Dajte samo ime Klijenta i podesiti koliko dana da bude važeći Vaš potpis.

```
/home/bin/openssl-openvpn-server-potpis-klijentu
```

### **Pošaljite Vaš paket Vašem Klijentu preko sigurne [SSH](#) veze.**

Ako se zagubi možete dobiti nepoželjan pristup u Vaš kompjuter.

### **Instalacija Certifikata kod Klijenta**

To mora da se uradi kod Klijenta!

Primili ste openvpn-klijent.tar.bz2 od Vašeg CA Server-a

U njemu se nalaze potpisani Certifikat i javni ključ

Otpakujte ga i prebacite sve u /etc/openvpn/keys/

Samo Vi smete da čitate taj potpisani Certifikat!

```
chmod 600 /etc/openvpn/keys/openvpn-klijent-cert.pem
```

Vaš direktorijum mora ovako da izgleda

```
ls -la /etc/openvpn/keys/
```

```
.  
..  
-rw----- 1 root root openvpn-ca.pem  
-rw----- 1 root root openvpn-klijent-cert.pem  
-rw----- 1 root root openvpn-klijent-key.pem  
-rw----- 1 root root ta.key
```

Javni ključ od Vašeg CA

openvpn-ca.pem

client1.crt, Client1 only, Client1 Certificate, No Secret  
Certifikat Klijenta. Samo kod klijenta.

openvpn-klijent-cert.pem

client1.key, Client1 only, Client1 Key, Yes Secret  
**Tajni ključ Klijenta.** Samo kod klijenta.

openvpn-klijent-key.pem

TLS key, this is used in handshaking

**Je tajni sigurnosni ključ. Svuda u mreži**

ta.key

**Instalacija Certifikata kod Servera**

To mora da se uradi na Serveru!

Kopirajte sa Vašeg CA kompjutera sledeće fajle. Slično kao i kod klijenta, samo što su ovo Vaši Certifikati, koje ste sami potpisali.

Nalaze se u Vašem CA

```
cd /etc/openvpn/CA
```

```
./openvpn-ca.pem  
.certs/openvpn-server-cert.pem  
.private/openvpn-server-key.pem
```

Napravite direktorijum

```
mkdir /etc/openvpn/keys
```

Uđite u taj direktorijum

```
cd /etc/openvpn/keys
```

Kopirajte iz Vašeg CA u /etc/openvpn/keys

```
cp -a /etc/openvpn/CA/openvpn-ca.pem ..../keys/  
cp -a /etc/openvpn/CA/certs/openvpn-server-cert.pem ..../keys/  
cp -a /etc/openvpn/CA/private/openvpn-server-key.pem ..../keys/
```

Sada treba napraviti Diffie-Hellman 2048 parametre u /etc/openvpn/keys

```
openssl dhparam -out dh2048.pem 2048
```

## Pravljenje TLS tajnog ključa

Za kraj treba napraviti TLS ključ, koji se koristi u procesu uspostavljanja veze.

On pravi ekstra sigurnost iznad normalne koju ima SSL/TLS, pravi "HMAC firewall", koji pomaže da blokira DoS napade i UDP Port napade "potope".

Uđite u direktorijum

```
cd /etc/openvpn/keys
```

Napravite tajni ključ

```
openvpn --genkey --secret ta.key
```

Proverite ga

```
openvpn --test-crypto --secret ta.key
```

I Server i Klijent moraju imati ovaj ključ.

Za Server

```
tls-auth /etc/openvpn/keys/ta.key 0
```

Za Klijente

```
tls-auth /etc/openvpn/keys/ta.key 1
```

Budite sigurni da su sve fajle sigurne i da pripadaju root-u

```
chown root:root *
```

```
chmod 600 *
```

Ovako otprilike treba da izgleda Vaš direktorijum sa Certifikatima i ključevima

```
ls -la /etc/openvpn/keys
```

```
drwx----- 2 .
drwxr-xr-x 4 ..
-rw----- 1 root root dh2048.pem
-rw----- 1 root root openvpn-ca.pem
-rw----- 1 root root openvpn-server-cert.pem
-rw----- 1 root root openvpn-server-key.pem
-rw----- 1 root root ta.key
```

Sve što treba da se uradi za Server i njegove Certifikate i ključeve radi ova fajla odjednom.

Vi morate samo pre toga da podesite prema [SSL protokol](#)

/etc/ssl/openssl.cnf

da ne pišete stalno iste podatke o Vašoj državi, mestu i ostalo.

Zapišite negde Vašu šifru koju morate ovde navesti više puta.

Trebaće Vam stalno kad budete potpisivali Certifikate klijenata.

/home/bin/openssl-openvpn-server

Ako želite da u Vašem CA napravite zahtev klijenta za potpis Certifikata i da ga odmah potpišete. Kad ga Klijent dobije mogao bi samo da ga otpakuje kod sebe u

/etc/openvpn/keys

/home/bin/openssl-openvpn-server-certifikat-i-potpis-klijentu

**Pošaljite Vaš paket Vašem Klijentu preko sigurne [SSH](#) veze.**

Potpisani Certifikat, tajni ključ klijenta, Server-ov javni ključ, TLS key.

Ako se zagubi možete dobiti nepoželjan pristup u Vaš kompjuter.

## Konfiguracije

Da vidite na koji način se možete povezati preko OpenVPN sa --auth opcijom, moraju da podržavaju i Server i Klijent.

```
openvpn --show-digests
```

Verovatno želite da koristite šifre. Da vidite koje šifriranje možete koristiti u OpenVPN sa --cipher opcijom, moraju isto da podržavaju i Server i Klijent.

```
openvpn --show-ciphers
```

Pokazuje hardwerske dodatke za šifrovanje (ako postoje)  
Show hardware crypto accelerator engines (if available).

```
openvpn --show-engines
```

Pokazuje sve vrste TLS šifrovanja (TLS se koristi samo za kontrolni kanal).

```
openvpn --show-tls
```

Napravite direktorijum za konfiguracije Vaših klijenata

```
mkdir /etc/openvpn/ccd
```

Uđite u taj direktorijum

```
cd /etc/openvpn/ccd
```

Napravite konfiguracionu fajlu za Vašeg klijenta i stavite u tu fajlu na primer

```
touch /etc/openvpn/ccd/IP-adresa-od-klijenta.com
```

```
# The Name of this File is Clients IP Address, static or dynamic.
```

```
#ifconfig-push clientIP serverIP  
ifconfig-push 192.168.100.2 192.168.100.1  
  
# http://www.secure-computing.net/wiki/index.php/OpenVPN/Routing  
iroute 192.168.2.0 255.255.255.0
```

Da proverite Vašu konfiguraciju

```
openvpn --config /etc/openvpn/Vaša-konfiguracija
```

[GNU/Linux Kernel](#) ovo normalno sam radi ako ste Device uključili u njegovoj konfiguraciji.

Sa ovom komandom možete probati napraviti Device ako je nemate.

```
openvpn --mktun --dev tun0
```

OpenVPN gleda normalno na

```
/dev/net/tun, /dev/tun, /dev/tap, etc.
```

Pokazuje šifrovani saobraćaj preko standardnog OpenVPN UDP Port-a

```
tcpdump -i eth0 udp port xxxxx
```

Pokazuje ne šifrovani sabraćaj preko TUN/TAP Device

```
tcpdump -i tun0
```

Vidite koje Device koristite sa

```
ifconfig
```

ili

**iwconfig**

## **strongSwan**

Free Software implementation of IPsec for the Linux operating system

Dodatak na VPN, Kernel Space, Free Software implementation of IPsec

<http://www.strongswan.org/>

emerge -a strongswan

## **KVpnc**

A KDE VPN connection utility

KDE GUI za OpenVPN

<http://home.gna.org/kvpnc/>

emerge -a kvpnc

## **CloudVPN**

Secure mesh networking VPN

<http://dev.e-x-a.org/projects/cloudvpn/wiki/>

<http://e-x-a.org/>

emerge -a cloudvpn

## **tinc**

An easy to configure VPN implementation

Dodatak na VPN, User Space, koristi RSA ključeve, nesigurno, samo jedan Developer

<http://www.tinc-vpn.org>

[http://www.gentoo-wiki.info/HOWTO\\_Setup\\_a\\_VPN\\_with\\_tinc](http://www.gentoo-wiki.info/HOWTO_Setup_a_VPN_with_tinc)

[http://www.linux-magazin.de/heft\\_abo/ausgaben/2003/10/einfache\\_verbindung](http://www.linux-magazin.de/heft_abo/ausgaben/2003/10/einfache_verbindung)

emerge -a tinc

/etc/init.d/tincd start

rc-update add tincd default

[Na početak](#)

## **Povezivanje pomoću tunela**

Imate više mogućnosti izaberite koja Vam odgovara za datu situaciju i Vaše potrebe.

<http://sistemac.carnet.hr/node/8>

## **HTTP tunnel**

Creates a bidirectional virtual data path tunnelled in HTTP requests. The requests can be sent via an HTTP proxy if so desired.

This can be useful for users behind restrictive firewalls. If WWW access is allowed through an HTTP proxy, it's possible to use htptunnel and, say, [Telnet](#) or PPP to connect to a computer outside the firewall.

Pravi tunel preko HTTP protokola, kroz zatvoren zaštitni zid.

<http://www.nocrew.org/software/htptunnel.html>

<http://www.gnu.org/software/htptunnel/>

Za [BSD](#)

portmaster -n www/htptunnel

## Za GNU/Linux

```
emerge -a httpstunnel
```

```
htc --help
```

```
hts --help
```

## **Stunnel**

The stunnel program is designed to work as SSL encryption wrapper between remote client and local (inetd-startable) or remote server. The concept is that having non- SSL aware daemons running on your system you can easily setup them to communicate with clients over secure SSL channel.

<http://stunnel.mirt.net>

<http://www.stunnel.org/>

## Za BSD

```
portmaster -n security/stunnel
```

## Za GNU/Linux

```
emerge -a stunnel
```

<http://www.stunnel.org/?page=docs>

<http://www.stunnel.org/?page=howto>

[http://www.mindspring.com/~joelmoses/demarc\\_stunnel.html](http://www.mindspring.com/~joelmoses/demarc_stunnel.html)

[http://www.gentoo-wiki.info/HOWTO\\_create\\_a\\_logserver\\_with\\_syslog-ng](http://www.gentoo-wiki.info/HOWTO_create_a_logserver_with_syslog-ng)

<https://bbs.archlinux.org/viewtopic.php?id=1306>

<http://wiki.cacert.org/StunnelConfiguration>

<http://etutorials.org/Linux+systems/secure+linux-based+servers/Chapter+5.+Tunneling/Section+5.1.+Stunnel+and+OpenSSL+Concepts/>

<http://www.linuxjournal.com/article/7628>

<http://linuxgazette.net/107/odonovan.html>

<http://www.bamafolks.com/randy/students/stunnel.pdf>

Ako hoćete da pravite chroot za [Stunnel](#)

<http://forums.fedoraproject.org/showthread.php?t=186431>

Može da se koristi za [NFS](#), [Rsync](#), [Synergy](#), [VNC](#), [SSVNC](#), [SSL/SSH VNC viewer](#), [syslog-ng](#), [HAProxy](#).

**Stunnel treba koristiti samo tamo gde ne možete da koristite SSH, koji je mnogo sigurniji i lakši za upotrebu.**

Da ga podignite

```
/etc/init.d/stunnel start
```

Da se automatski podigne pri startanju sistema

```
rc-update add stunnel default
```

**Ako hoćete veliku sigurnost i da se niko ne može ulogovati, ako nema Vaš certifikat.**

**Koristite za prenos samo sigurne veze na primer [scp](#), [FTP](#), [elektronsku poštu](#) zaštićenu sa [GnuPG](#), [Jabber](#) sa [OTR](#)...**

Naizmenično na kompjuterima Vaših sagovornika, certifikati se moraju potpisivati i vraćati, dakle sve po redu jedno po jedno. Prvo jedan korak kod oba pa tek onda sledeći. Koliko god da imate korisnika morate to da ponovite.

Trebate napraviti ključeve na serveru za [Stunnel](#) na primer sa

```
/home/bin/openssl-stunnel1-server
```

Pošaljite taj Certificat Request sa servera klijentu na potpis.

Potpisite Certificat Request na klijentu na primer sa

```
/home/bin/openssl-stunnel2-signed-back
```

Pošaljite potpisani Certificat nazad na Vaš server.

Napravite finalni proizvod hostname.pem za Vaš server.

```
/home/bin/openssl-stunnel3-certificate
```

Ako hoćete da sami potpišete certifikate, što je lako, ali nije nikako sigurno, jer tu nema nikakve prave provere. Gleda se samo da li postoji certifikat i ništa više.

```
/home/bin/openssl-stunnel-self-signed
```

Podesite na serveru

/etc/stunnel/stunnel.conf

```
...
[klijent-nfs]
accept = localhost:2049
connect = ip-adresa:drugi-viši-port
cert = /etc/stunnel/hostname-klijent.pem
#client=yes
```

```
[klijent-rsync]
accept = localhost:873
connect = ip-adresa:drugi-viši-port
cert = /etc/stunnel/certs/hostname-klijent.pem
#client=yes
```

Podesite na klijentu

/etc/stunnel/stunnel.conf

```
...
[klijent-nfs]
accept = localhost:2049
connect = ip-adresa:drugi-viši-port
cert = /etc/stunnel/hostname-klijent.client.pem
client=yes
```

```
[klijent-rsync]
accept = localhost:873
connect = ip-adresa:drugi-viši-port
cert = /etc/stunnel/certs/hostname-klijent.client.pem
client=yes
```

Podignite ga sa

```
/etc/init.d/stunnel start
```

Da se stalno podigne pri dizanju sistema

```
rc-update add stunnel default
```

Da vidite šta se dešava, da li se koriste certifikati i adrese

```
strace stunnel
```

## **Proxtunnel**

A program that connects stdin and stdout to an origin server somewhere in the Internet through an industry standard HTTPS proxy.

<http://proxytunnel.sourceforge.net/>

Za [BSD](#)

```
portmaster -n security/proxytunnel
```

Za [GNU/Linux](#)

```
emerge -a proxytunnel
```

## **VTtun, Virtual Tunnel**

Provides the method for creating Virtual Tunnels over TCP/IP networks and allows to shape, compress, encrypt traffic in that tunnels.

Pravi virtuelne tunele preko TCP/IP protokola sa šifrovanjem i kompresijom

<http://vtun.sourceforge.net>

Za [BSD](#)

```
portmaster -n net/vtun
```

Za [GNU/Linux](#)

```
emerge -a vtun
```

## **Zebedee**

Is a simple program to establish an encrypted, compressed TCP/IP "tunnel" between two systems. This allows TCP-based traffic such as [Telnet](#), ftp and X to be protected from snooping as well as potentially gaining performance over low-bandwidth networks from compression.

Malo stariji program

<http://www.winton.org.uk/zebedee/>

Za [BSD](#)

```
portmaster -n security/zebedee
```

Za [GNU/Linux](#)

```
emerge -a zebedee
```

## **Dnsmasq**

Small forwarding DNS server

<http://www.thekelleys.org.uk/dnsMasq/doc.html>

Za [BSD](#)

```
portmaster -n dns/dnsmasq
```

Za [GNU/Linux](#)

```
emerge -a dnsmasq
```

## IMspecto

Is an [Instant Messaging](#) proxy with monitoring, blocking and content-filtering capabilities. Currently it supports MSN, Jabber/XMPP, AIM, ICQ, Yahoo, IRC and Gadu-Gadu to different degrees. MSN is the principle protocol, as it's the most popular these days, at least in the UK where I'm based. The supported platforms are at present Linux and BSD when using the [PF](#) firewall, but porting to other UNIXs should be trivial. It is able to log to plain files, as well as several types of SQL database including MySQL, SQLite and PostgreSQL.

<http://www.imspector.org/wordpress/>

Postoji kao [PfSense paket](#).

Za [BSD](#)

```
portmaster -n net-im/imspector
```

[Povezivanje pomoću tunela](#)

[HTTP tunnel](#)

[Stunnel](#)

[VTtun, Virtual Tunnel](#)

[Zebedee](#)

[Dnsmasq](#)

[IMspecto](#)

[Na početak](#)

## **Povezivanje preko X protokola**

Ima puno načina da delite Vaš X, monitor, tastaturu i miša, izaberite šta Vam odgovara.

[https://en.wikipedia.org/wiki/Multiseat\\_configuration](https://en.wikipedia.org/wiki/Multiseat_configuration)

**Ako imate više kompjutera a jednu tastaturu i jednog miša**

I ne želite da imate više tastatura i miševa i da se stalno prebacujete sa jedne na drugu jedinicu.

Više kompjutera možete probati da upravljate bez dodatnih aparata kao [KVM uređaja](#) ili sličnih uređaja, mada su oni najbolji ako se radi u lokalu.

Ovi programi mogu samo da Vam prebace tastaturu i miša, a šta je ako imate više kompjutera, a samo jedan monitor?

To možete lako rešiti, ako imate više priključaka na monitoru i odgovarajuće priključke na Vašim grafičkim kartama. Onda samo na monitoru prebacujte ulaz koji se koristi.

Možete koristiti VGA, DVI, HDMI, DP priključke, to jeste šta god imate i odgovara Vašem monitoru i [grafičkim kartama](#).

Prvo proverite da li Vam X podržava Xtest eksenziju, bez nje neće raditi

```
xdpyinfo | grep XTEST
```

Možete koristiti i [VNC protokol](#), ali on zauzima više resursa Vaše mreže, CPU, slika može da bude lošija. Ali ako imate samo jedan monitor [VNC protokol](#) je bolji za sada.

## Synergy

Synergy lets you easily share a single mouse and keyboard between multiple computers with different operating systems, each with its own display, without special hardware. It's intended for users with multiple computers on their desk since each system uses its own display.

All you need is a LAN connection.

It's intended for users with multiple computers, where each system uses its own display.

Synergy+ and Synergy have now merged!

<http://synergy-foss.org/>

<http://synergy-foss.org/pm/projects/synergy/wiki/RelatedProjects>

Stare stranice

<http://synergy2.sourceforge.net/>

<http://code.google.com/p/synergy-plus/>

Da vidite šta sve ima za [Synergy](#)

## Za BSD

```
find /usr/ports/* | grep synergy
```

## Za GNU/Linux

```
eix synergy
```

```
eix -S synergy
```

<http://synergy-foss.org/pm/projects/synergy/tabs/download>

## Za BSD

```
portmaster -n sysutils/synergy
```

## Za GNU/Linux

Možda promeni ime za ebuild pa dotle može da se ručno instalije, posebno ako hoćete nove verzije.

```
emerge -a synergy-plus
```

Možete skinuti sa ovom skriptom

/home/bin/svn/svn-Synergy

Možete instalisati sa ovom skriptom, zajedno sa [QSynergy](#)

/home/bin/install-synergy

<https://groups.google.com/forum/#!forum/synergy-plus>

<http://en.gentoo-wiki.com/wiki/Synergy>

<http://en.wikipedia.org/wiki/Synergy%2B>

[https://secure.wikimedia.org/wikipedia/en/wiki/Synergy\\_%28software%29](https://secure.wikimedia.org/wikipedia/en/wiki/Synergy_%28software%29)

<http://lugons.org/Uputstva/Opste/kako-podesiti-synergy>

<http://www.linux.com/archive/feed/54628>

<http://lifehacker.com/#!254648/hack-attack-control-multiple-computers-with-a-single-keyboard-and-mouse>

<http://www.lifehacker.com.au/2011/02/how-to-control-multiple-computers-with-a-single-keyboard-and-mouse/>

**Trebate Synergy konfigurisati samo na serveru, to Vam ne treba na klijentu.**

Za sada prenosi Synergy podatke nešifrovano, što je veoma nesigurno.

Možete koristiti SSH za prenos, dok ne dođe neka nova verzija koja ima zaštitu već u sebi

<http://synergy2.sourceforge.net/security.html>

<http://synergy-foss.org/pm/issues/13>

Možete koristiti Synergy sa Stunnel

<http://www.stunnel.org/?page=docs>

[http://home.arcor.de/lightsky/docs/stunnel\\_openssl\\_synergy.pdf](http://home.arcor.de/lightsky/docs/stunnel_openssl_synergy.pdf)

Kako da na smopu!M promenite Monitor sa Synergy, može se preneti na BSD i GNU/Linux

<http://bytes.com/topic/windows/answers/683922-possible-switch-monitor-input-analog-digital-programmatically>

## QSynergy

A comprehensive and easy to use graphical front end for Synergy

GUI za Synergy

<http://www.volker-lanz.de/en/software/qsynergy/>

Postoji i eksperimentalni Ebuild za Gentoo na

[https://bugs.gentoo.org/show\\_bug.cgi?id=234673](https://bugs.gentoo.org/show_bug.cgi?id=234673)

Ebuild dodajte u lokalni Overlay

emerge -a qsynergy

## **QuickSynergy**

[GUI](#) for configuring and running [Synergy](#)

[GUI](#) za [Synergy](#)

<http://quicksynergy.sourceforge.net/>

Postoji novija QuickSynergy verzija na Stranici, [ručno se instalije](#)

Za [BSD](#)

portmaster -n sysutils/quicksynergy

Za [GNU/Linux](#)

Dodajte Overlay [Sunrise](#) za [QuickSynergy](#)

emerge -a quicksynergy

## **X2X**

An utility to connect the Mouse and KeyBoard to another X

<http://www.the-labs.com/X11/#x2x>

emerge -a x2x

Ima i git verzija

<https://github.com/dottedmag/x2x>

Za [BSD](#)

portmaster -n x11-servers/x2x

Za [GNU/Linux](#)

Možete skinuti sa

/home/bin/git/git-X2X

Možete instalisati sa

/home/bin/ install-x2x

Pročitajte Manual

ssh -X drugi-kompjuter x2x -east -to :0

Njegov protokol koristi i x2vnc.

Ovde imate dobre primere kako da koristite X2X sa SSH.

Obavezno dobro proučite zbog sigurnosti.

<http://www.linuxjournal.com/content/share-keyboardmouse-between-multiple-computers-x2x>

<http://www.linux.com/archive/feature/148824>

## Mango Lassi

Share mouse and pointer with other Computers.

Something like a Synergy done right, or an X2X that doesn't suck.

<http://0pointer.de/blog/projects/mango-lassi.html>

<http://github.com/herzi/mango-lassi>

<http://mango-lassi.sourceforge.net/about/>

Instališe se ručno.

Možete skinuti sa

/home/bin/git-Mango-Lassi

Možete instalirati sa

/home/bin/install-mango-lassi

[Povezivanje preko X protokola](#)

[Ako imate više kompjutera a jednu tastaturu i jednog miša](#)

[Synergy](#)

[OSynergy](#)

[QuickSynergy](#)

[X2X](#)

[Mango Lassi](#)

[Preko SSH protokola na udaljeni X](#)

[VNC protokol, Virtual Network Computing](#)

[NX protokol](#)

[Linux Terminal Server Project](#)

[RDP protokol, Remote Desktop Protokol](#)

[GUI za razne protokole](#)

[Ostala rešenja za povezivanje preko X protokola](#)

[Na početak](#)

Šta sve postoji

[http://en.wikipedia.org/wiki/Comparison\\_of\\_remote\\_desktop\\_software](http://en.wikipedia.org/wiki/Comparison_of_remote_desktop_software)

[http://www.trojaner-und-sicherheit.de/tcp\\_ip\\_und\\_internet/tunneling\\_protokolle.htm](http://www.trojaner-und-sicherheit.de/tcp_ip_und_internet/tunneling_protokolle.htm)

## **Preko SSH protokola na udaljeni X**

<http://en.gentoo-wiki.com/wiki/X-Forwarding>

[http://www.gentoo-wiki.info/HOWTO\\_X-forwarding](http://www.gentoo-wiki.info/HOWTO_X-forwarding)

<http://www.vanemery.com/Linux/XoverSSH/X-over-SSH2.html>

<http://www.linux-tip.net/cms/content/view/302/26/>

Na primer možete ovako

ssh -f -X -p Vaš-Port -i ~/.ssh/user\_dsa user@server /home/bin/startx-1

[Normalno možete startati i više X sesija na udaljenom računaru.](#)

## **VNC protokol, Virtual Network Computing**

<http://www.howtoforge.com/creating-a-jail-with-vnc-server-on-freebsd>

<http://en.gentoo-wiki.com/wiki/X11VNC>

[http://en.gentoo-wiki.com/wiki/XVNC\\_Server](http://en.gentoo-wiki.com/wiki/XVNC_Server)

<https://help.ubuntu.com/community/VNC>

<http://www.vanemery.com/Linux/VNC/vnc-over-ssh.html>

<http://www.linuxjournal.com/article/5499>

<http://www.linuxjournal.com/node/5560/>

[http://www.ns-linux.org/Uputstva/Opste/Tunnelling\\_x11vnc\\_via\\_ssh/](http://www.ns-linux.org/Uputstva/Opste/Tunnelling_x11vnc_via_ssh/)

[https://en.wikipedia.org/wiki/Virtual\\_Network\\_Computing](https://en.wikipedia.org/wiki/Virtual_Network_Computing)

<http://linuxtutorialvideos.blogspot.com/2009/01/remote-loginvncssh.html>

Dosta dobrih informacija

<http://faq.gotomyvnc.com/>

Kod sporijih veza je brži NX protokol, jer koristi kompresiju.

Predlaže se na mnogo stranica da se koriste lakši Window Manager-i i Desktop okruženja.

Jer prenosi se puno slika i detalja, pa to usporava VNC vezu. Možete probati da iskjučite kompresiju za JPEG slike. Mada je najbolje da se koriste samo Window Manager-i.

Da vidite šta ima

Za BSD

```
find /usr/ports/* | grep vnc
```

```
grep -r vnc /usr/ports/net
```

Za GNU/Linux

```
eix vnc
```

```
eix -S vnc
```

## **x11vnc**

Is a VNC server for real X displays. VNC (Virtual Network Computing) is a very useful network graphics protocol which allows multiple simple remote viewers to watch and control a single desktop. x11vnc differs from traditional UNIX VNC servers in that it is accessing a real X displays that may already be in progress rather than creating its own X server for clients to connect to.

Znači koristi Vaše normalno [grafičko okruženje](#), što je za pohvalu, jer onda radite u Vašem omiljenom okruženju.

Odlično radi kao Server, veoma sam zadovoljan sa [x11vnc](#).

Može da radi zajedno sa klijentima [SSVNC](#), [TightVNC](#), [TigerVNC](#) veoma veliki [FAQ](#), vredi pročitati, kao i ovu celu stranicu.

<http://www.karlrunge.com/x11vnc/>

<http://en.gentoo-wiki.com/wiki/X11VNC>

Za [BSD](#)

```
portmaster -n net/x11vnc
```

Za [GNU/Linux](#)

```
emerge -a x11vnc
```

```
x11vnc -opts
```

```
x11vnc -help
```

```
man x11vnc
```

## **TightVNC**

A free remote control software package

Enhanced version of VNC, called TightVNC (grown from the VNC Tight Encoder project), which is optimized to work over slow network connections such as low-speed modem links. While original VNC may be very slow when your connection is not fast enough, with TightVNC you can work remotely almost in real time in most environments. Besides bandwidth optimizations, TightVNC also includes many other improvements, optimizations and bugfixes over VNC. Note that TightVNC is free, cross-platform and compatible with the standard VNC.

Klijent i Server za grafički login na drugi kompjuter.

Zamena za [RealVNC](#), koji više ne razvija [Free Software](#) verziju.

Ima i novija verzija za [smopu!M](#) sa dodacima da bi bolje radila grafika.  
[TigerVNC](#) je to odlično rešio.

<http://www.tightvnc.com>

Za [BSD](#)

```
portmaster -n net/tightvnc
```

Za [GNU/Linux](#)

```
emerge -a tightvnc
```

<http://www.freebsddiary.org/tightvnc.php>

Izvršne fajle su

```
Xvnc
```

```
vncconnect
```

```
vncpasswd
```

```
vncserver
```

Komanda za normalni vncviewer je

```
vncviewer
```

## TigerVNC

Remote desktop viewer display system

Odličan nastavak od [TightVNC](#), koji više razvija [smopu!M](#) verziju.

[TurboVNC](#) se utopio u [TigerVNC](#). Koristi [libjpeg-turbo](#).

Radi odlično kao klijent, veoma lepa OpenGL grafika. Na primer sa Fullscreen-u se mogu u kombinaciji sa [x11vnc](#) u [Fluxbox](#)-u videti slit, prebacivati prozori...

Ako se koristi kao Server onda ima svoje [grafičko okruženje](#), što ne želi svako.

Možete svako grafičko okruženje da koristite.

Radi odlično sa SSH Tunnel za VNC i SSL Tunnel za VNC.

<http://www.tigervnc.org/>

<http://sourceforge.net/apps/mediawiki/tigervnc/>

Za BSD

Instališe se ručno.

Za GNU/Linux

emerge -a tigervnc

man vncviewer

<http://www.virtualgl.org/About/TigerVNC>

<http://fedoraproject.org/wiki/Features/TigerVNC>

<http://www.virtualgl.org/>

Komanda za normalni vncviewer je

vncviewer

## **SSVNC, SSL/SSH VNC viewer**

VNC viewer that adds encryption security to VNC connections

The Enhanced TightVNC Viewer, SSVNC, adds encryption security to VNC connections

<http://www.karlrunge.com/x11vnc/ssvnc.html>

Za BSD

Bolje je da trenutno da ručno instalirate sa

cd /usr/ports/net/ssvnc ; make install clean

nego sa

```
portmaster -n net/ssvnc
```

## Za [GNU/Linux](#)

```
emerge -a ssvnc
```

Default je mala slika, lošije boje.

Da bi se mogao instalirati mora se koristiti [Oracle JDK](#), može sa [Oracle JRE](#)

Možete koristiti [SSVNC, SSL/SSH VNC viewer](#) sa [Stunnel \(SSL Tunnel za VNC\)](#) i [SSH Tunnel za VNC](#).

[http://www.karlrunge.com/x11vnc/ssvnc\\_help.html](http://www.karlrunge.com/x11vnc/ssvnc_help.html)

Izvršne fajle su

```
ssvnc-gui
```

```
man ssvnc-gui
```

```
ssvnc-ts
```

```
ssvnc-stunnel
```

## Za [GNU/Linux](#)

```
ssvnc --help
```

Komanda za normalni vncviewer je

```
ssvncviewer
```

```
man ssvncviewer
```

```
ssvncviewer --help
```

Da imate Vaša stalna podešavanja treba da imate ovu fajlu

```
~/ssvncrc
```

Certifikat Servera ste već verovatno sa ovim [programom uvezli](#), navedite koji je Certifikat klijenta i ostale potrebne parametre kao VNC šifru.

VNC Host:Display

```
Stavite tu IP-adresa:VNC-Port
```

Kada ste uspešno ostvarili SSL sesiju osigurajte je sa Save na primer sa imenom

```
IP-adresa-VNC-Port-ssl.vnc
```

Tako ćete uvek da znate koji se protokol, IP adresa i Port koristi.

Možete promeniti koji vncviewer koristite, dajte punu putanju do programa

```
Ctrl+a / Change VNC Viewer
```

Naravno možete ista podešavanja da zapamtite pod drugim imenima dodato samo ime Vašeg Viewera

Da vidite koje profile imate zapamćene

```
ssvnc -profiles
```

```
IP-adresa-VNC-Port-ssl  
IP-adresa-VNC-Port-ssl-tigervnc
```

## **ss\_vncviewer**

Wrapper for vncviewer to use an stunnel SSL tunnel or an [SSH Tunnel](#).

Možete skinutu ovu skriptu, koja pokušava da vncviewer koristi [Stunnel](#) SSL tunnel ili [SSH Tunnel](#). Radi odlčno sa [x11vnc sa SSL podrškom za Certificate Servera i klijenata](#).

[http://www.karlrunge.com/x11vnc/faq.html#ss\\_vncviewer](http://www.karlrunge.com/x11vnc/faq.html#ss_vncviewer)

```
cd /home/bin  
wget http://www.karlrunge.com/x11vnc/ss_vncviewer  
chmod +x ss_vncviewer
```

Možete staviti da se [automatski obnavlja](#).

## Vinagre

VNC Client for the [Gnome](#) Desktop

Ima malo problema sa stabilnošću i slikom. Zna da zakoči i drugi kompjuter.

<http://projects.gnome.org/vinagre/>

Za [BSD](#)

```
portmaster -n net/vinagre
```

Za [GNU/Linux](#)

```
emerge -a vinagre
```

## gtk-vnc

Is a VNC viewer widget for GTK+. It is built using coroutines, allowing it to be completely asynchronous while remaining single threaded. It supports RFB protocols 3.3 through 3.8 and the VeNCrypt authentication extension providing SSL/TLS encryption with x509 certificate authentication. The core library is written in C and a binding for Python using PyGTK is available. The networking layer supports connections over both IPv4 and IPv6. Example code illustrates how to build a vncviewer replacement using either C or Python.

<http://live.gnome.org/gtk-vnc>

Za [BSD](#)

```
portmaster -n net/gtk-vnc
```

Za [GNU/Linux](#)

```
emerge -a gtk-vnc
```

## x2vnc

Control a remote computer running [VNC](#) from X, a dual-screen hack

Koristi kod od [X2X](#) i [VNC](#), dobra kombinacija.

Ima i [Win2VNC](#) za smopu!M sa istim kodom

<http://fredrik.hubbe.net/x2vnc.html>

Za [BSD](#)

```
portmaster -n x11-servers/x2vnc
```

Za [GNU/Linux](#)

```
emerge -a x2vnc
```

## iTALC

Intelligent Teaching And Learning with Computers (iTALC) supports working with computers in school

Koristi [VNC](#), može da se koristi za škole, kao i [LTSP](#).

<http://italc.sourceforge.net/>

Za [GNU/Linux](#)

```
emerge -a italc
```

## [VNC](#) alatke

### VNCcrack

Is a fast offline password cracker for [VNC](#) passwords. By sniffing a [VNC](#) challenge-response sequence off the network (typically when [VNC](#) is used without a decent cryptographic wrapper like SSH or SSL), you can recover the password fairly easily and quickly by letting

VNCcrack pound on it.

<http://www.randombit.net/code/vnccrack/>

Za [BSD](#)

portmaster -n security/vnccrack

## vnc2flv

Is a cross-platform screen recording tool for UNIX, Windows or Mac. It captures a [VNC](#) desktop session (either your own screen or a remote computer) and saves as a Flash Video (FLV) file.

<http://www.unixuser.org/~euske/python/vnc2flv/>

Za [BSD](#)

portmaster -n deskutils/vnc2flv

## Upotreba [VNC](#)-a

**Nemojte koristiti [VNC protokol](#) kao [root](#), nego samo kao [normalni korisnik](#) zbog sigurnosti i da možete imate Vaše normalno i [grafičko okruženje](#).**

**Kad je ostvarena veza menu je F8. Zavisno od klijenta imate drukčije opcije.**

Ako želite samo pojedine aplikacije pokrenuti na Serveru možete za to koristiti [xpra](#).

Postoji podprogram iz paketa [Avahi](#) koji može da proveri koji [VNC](#) Server je podignut i da se proba na njega konektovati.

bvnc

Da vidite da li ste spolja dostupni preko [VNC protokol](#)-a

Mada ovo javlja skoro uvek da ste dostupni preko Portova 5900 do 5909, iako ih niste možda uopšte dopustili ili koristite [programe za sakrivanje IP adrese](#).

<http://www.gotomyvnc.com/>

Pogledajte [Podešavanja xorg.conf](#)

Da bi se podigao dodatak za [VNC](#) i da bi imali učitano VncAuth.

Bolje je da se ne učitava taj dodatak, već da se koristi pravi Server na primer [x11vnc](#).  
Ako imate greške kod konektovanja probajte uključiti vnc dodatak.

<http://wiki.centos.org/HowTos/VNC-Server>

/etc/X11/xorg.conf

Section "Module"  
...

    Load "vnc"

EndSection

Section "Screen"  
...

    Option "SecurityTypes" "VncAuth"

    Option "UserPasswdVerifier" "VncAuth"

    Option "PasswordFile" "/home/VNC-user/.vnc/passwd"

EndSection

Ako ne postoji napravite direktorijum

mkdir ~/.vnc

**Morate imati [VNC](#) šifru zbog sigurnosti**

<http://www.karlrunge.com/x11vnc/faq.html#faq-passwdfile>

**To morate imati da ne bi svako mogao da su tek tako uloguje kod Vas preko [VNC](#) protokola.**

Za [x11vnc](#)

x11vnc -storepasswd ~/.vnc/passwd

ili sa [TightVNC](#) ili [TigerVNC](#)

```
vncpasswd
```

Možete imati i takozvanu view-only šifru sa kojom ne može da se kontroliše Vaš kompjuter.

```
~/.vnc/passwd
```

```
normalna-VNC-šifra
```

```
__BEGIN_VIEWONLY__
```

```
view-only-šifra
```

## **Samo za probu da li radi [VNC](#)**

Startajete da bi ostvarili sesiju, to je bez zaštite, samo za probu u lokalu.

Možete automatski dobiti pun ekran ako uzmete opciju -fullscreen

Zavisno od verzije Viewer-a imate različite opcije.

Za [TigerVNC](#)

```
vncviewer -passwd /home/VNC-user/.vnc/passwd server:display
```

```
vncviewer -passwd /home/VNC-user/.vnc/passwd server:Viši-port
```

Za [SSVNC](#)

```
ssvncviewer -passwd /home/VNC-user/.vnc/passwd server:display
```

```
ssvncviewer -passwd /home/VNC-user/.vnc/passwd server:Viši-port
```

Možete startati [SSH Tunnel](#) i onda pokrenuti ako već niste VNC server na primer sa

```
x11vnc >> ~/.x11vnc.log 2>&1 &
```

ili sa skriptom

```
/home/bin/vncserver-
```

Možete na klijentu startati da čeka na signal Servera

```
vncviewer -passwd /home/VNC-user/.vnc/passwd -listen
```

Onda treba na Serveru da se izvrši

```
x11vnc -connect IP-adresa-klijenta
```

ili sa skriptom

```
/home/bin/vncserver-connect IP-adresa-klijenta
```

## Koje sve Servere možete sa VNC imati

Možete koristiti i normalnog korisnika kao VNC-user-a, što je za razmišljanje, jer donosi mnoge sigurnosne probleme.

**Pažnja radite samo sa VNC u lokalnu i obavezno imajte  
SSH Tunnel za VNC i SSL Tunnel za VNC dobro nameštene, sve proverite više  
puta, da ne bi imali napada na normalno nezaštićenom VNC.**

**Tek kad to dobro u lokalnu ispitate, možete sa Interneta, preko svojih dinamičkih  
IP adresa probajte sami sebi da se ulogujete i sve ponovo ispitate.**

**Tek kad ste potpuno sigurni, možete ići dalje korake, da neki u koga ste sigurni  
proba da se kod Vas ili Vi kod njega ulogujete sa zaštićenim VNC.**

Obratite pažnju da možete koristiti na istom realnom Display :0 sa x11vnc samo jedan Port i to na primer \*\*\*0.

Tako da možete u tom slučaju imati samo SSH Tunnel za VNC ili SSL Tunnel za VNC na jednom Port-u.

Naravno možete imati različite konfiguracije za x11vnc to jest različite Portove za SSH Tunnel za VNC i SSL Tunnel za VNC.

Za probu sam ih sva četiri VNC Servera istovremeno startao plus jedan X za Display :0 na klijentu, samo za igre.

Možete imati x11vnc VNC Server, Display :0, VNC-Port \*\*\*0, SSH Tunnel za VNC

Možete imati x11vnc VNC Server, Display :0, VNC-Port \*\*\*\*1, [SSL Tunnel za VNC](#)

Možete koristiti normalni VNC Server, Display :2, VNC-Port \*\*\*\*2

Možete imati Frame Buffer Display, Display :3, VNC-Port \*\*\*\*3

Možete videti da li Vam je podignut X sa

```
ps wwaux | grep X
```

### Možete koristiti normalni VNC server

Ako se ne koristi [x11vnc](#) nego neki drugi Server na primer [TigerVNC](#), onda ćete dobiti [grafičko okruženje](#), koje je definisano u

```
~/.vnc/xstartup
```

Možete svako [grafičko okruženje](#) da koristite. Default je [twm](#).  
Namestio sam da se koristi [Fluxbox](#).

Možete na Serveru startati na primer [TigerVNC](#) sa

```
vncserver -rfbport ****2 -geometry 1920x1200 -desktop Xvnc
```

Ili sa ovom skriptom

```
/home/bin/vncserver-xvnc
```

Onda na klijentu startajta na promer [TigerVNC](#) sa

```
vncviewer -passwd /home/VNC-user/.vnc/passwd -fullscreen IP-adresa:****2
```

Ili sa ovom skriptom

```
/home/bin/vncviewer-xvnc IP-adresa
```

## **Možete imati Frame Buffer Display**

Koji ne koristi grafičku kartu i samo je u memoriji.

Pokrenite na Serveru na primer na trećem displeju

```
Xvfb :3
```

Onda pokrenite [x11vnc](#) sa višim Portom koji odgovara displeju

```
x11vnc -display :3 -rfbport ****3
```

Mada to možete uraditi u samo jednom koraku

```
x11vnc -create -display :3 -rfbport ****3
```

Onda se možete sa klijenta ulogovati na primer sa [TigerVNC](#)

```
vncviewer -passwd /home/VNC-user/.vnc/passwd -fullscreen IP-adresa:****3
```

Ili sa skriptom

```
/home/bin/vncviewer-xvfb IP-adresa
```

Možete i [konzolu](#) koristiti sa

```
x11vnc -rawfb console
```

```
x11vnc -rawfb vt1
```

## **Možete imati [x11vnc](#) VNC Server**

[x11vnc](#) koristi Vaše normalno [grafičko okruženje](#), što je za pohvalu, jer onda radite u Vašem omiljenom okruženju, koje je već startano.

## Možete imati različite konfiguracije za x11vnc

Trebate da imate ovu važnu fajlu sa opcijama koji x11vnc stalno koristi

```
~/.x11vncrc
```

Možete imati različite Portove za SSH Tunnel za VNC i SSL Tunnel za VNC.

Konfiguracije su potpuno iste samo se Portovi i imena sesija razlikuju

```
~/.x11vncrc-*
```

Uđite u Vaš VNC direktorijum

```
cd /home/VNC-user
```

Kopirajte i promenite ime za ~/x11vncrc

```
cp -a .x11vncrc .x11vncrc-ssl  
mv .x11vncrc .x11vncrc-ssh
```

Možete linkovati, onu konfiguraciju koju najviše koristite na primer sa

```
ln -s .x11vncrc-ssh .x11vncrc
```

Pa ako ne zovete sa -rc opcijom imate ipak svoju konfiguraciju

Odsada zovite x11vnc na primer sa

Da bi mogli koristiti SSH Tunnel sa VNC

```
x11vnc -rc ~/.x11vncrc-ssh ...
```

## Da bi mogli koristiti SSL Tunnel sa VNC

```
x11vnc -rc ~/x11vncrc-ssl ...
```

## **Ako imate problema da startate x11vnc ili TigerVNC Serverom**

<http://www.karlrunge.com/x11vnc/faq.html#faq-xperms>

Možete da vidite koji Display koristite sa

```
echo $DISPLAY
```

Normalno je to

```
:0.0
```

Ako dobijete greške na primer tipa da ne možete dobiti Display

```
XOpenDisplay(":0") failed.  
keyInvalid MIT-MAGIC-COOKIE-1
```

Probajte da koristite ovu opciju dodatno sa ostalim opcijama

[http://www.karlrunge.com/x11vnc/x11vnc\\_opts.html#opt-find](http://www.karlrunge.com/x11vnc/x11vnc_opts.html#opt-find)

**x11vnc -find** ostale-opcije

A ako Vam x11vnc pri startanju javlja da je Port koji koristite zauzet

```
Error: could not obtain listening port.
```

Znači da je već podignut x11vnc ili neki drugi VNC Server na tom Portu.

Prvo probajte selektivno da nađete i ubijete taj program koji je zauzeo Port sa

htop

Možete probati da ubijete taj VNC Server naravno na Serveru sa, ali šta ako imate više sesija sa različitim opcijama za x11vnc, sve onda morate ponovo startati

killall x11vnc

Pa da ponovo startate x11vnc sa opcijama koje Vam odgovaraju za određeni postupak.

Naravno uvek imate mogućnost da restartujete X na Server-u, ali to je zadnja mogućnost, ako ništa ne radi više.

### **Možete imati GUI za x11vnc**

<http://www.karlrunge.com/x11vnc/faq.html#faq-config-file>

x11vnc -gui

Da imate GUI za x11vnc System Tray sa opcijama

x11vnc -gui tray

### **Da možete x11vnc zaustaviti**

Da zaustavite x11vnc

x11vnc -R stop

Da sve klijente isključite sa Server-a x11vnc

x11vnc -R disconnect:all

## **Da bi mogli koristiti SSH Tunnel sa VNC**

<http://www.karlrunge.com/x11vnc/#tunnelling>

<http://www.vanemery.com/Linux/VNC/vnc-over-ssh.html>

<http://www.commandlinefu.com/commands/tagged/1064/ssh-tunnel>

<http://wiki.ubuntuusers.de/VNC>

Možete da ostvarite SSH Tunnel i da startate na primer TigerVNC.

Možete koristi TigerVNC vncviewer specijalnu opciju -via za gateways.

Radi odlično, iz prve možete imati drugi X na klijent ekranu.

Pravi SSH Tunnel i pokreće na primer x11vnc sa, to je jedna linija

```
ssh -p SSH-Port -i ~/.ssh/privat_dsa -X -f -t -L VNC-Port:localhost:VNC-Port $1 'killall x11vnc && x11vnc -rc ~/.x11vncrc-ssh -find -localhost >> ~/.x11vnc-ssh.log 2 >&1 &'
```

ili skripta

```
/home/bin/vncviewer-ssh-tunnel
```

Onda na drugoj konzoli startajte na primer TigerVNC sa, to je jedna linija

```
vncviewer -passwd /home/normalni-korisnik/.vnc/passwd -name SSH -fullscreen -via IP-adressa localhost
```

Ili skripta

```
/home/bin/vncviewer-local-ssh IP-adresa
```

Bolje i čistije je posebno startate SSH Tunnel i vncviewer-a, prema gornjim primerima.

Pravi SSH Tunnel, starta x11vnc i na kraju pokreće TigerVNC

```
/home/bin/vncviewer-ssh-all IP-adresa
```

Ostaje ovaj [SSH Tunnel](#), pa se može koristiti za dalju upotrebu

```
x11vnc -rc ~/.x11vncrc-ssh -find -localhost
```

Pravi [SSH Tunnel](#), malo komplikovano. Koristi [ss\\_vncviewer](#) i [TigerVNC](#).

```
/home/bin/vncviewer-ss-ssh-tunnel IP-adresa
```

Ostaje ovaj [SSH Tunnel](#), pa se može koristiti za dalju upotrebu

```
x11vnc -rc ~/.x11vncrc-ssh -find -localhost
```

Možete proveriti da li imate SSH ili SSL tunel i da li se koristi na primer sa

```
netstat -an | grep IP-adresa
```

## Da bi mogli koristiti [SSL Tunnel](#) sa [VNC](#)

**Možete koristiti za malo korisnika [Stunnel](#) certifikate, koje ste verovatno već napravili, ali znajte da ti certifikati nisu podešeni za [VNC](#).**

**Pazite modusi šifrovanja VeNCrypt, ANONTLS, i "ANON" nisu podržani u -stunnel modusu.**

**To je samo modus koji se podržava, zaostatak iz prošlosti.**

[http://www.karlrunge.com/x11vnc/x11vnc\\_opts.html#opt-stunnel](http://www.karlrunge.com/x11vnc/x11vnc_opts.html#opt-stunnel)

**Ako imate mnogo korisnika, onda napravite prema ovim stranicama i [Stunnel](#) primerima Vaše Certificate samo za [VNC](#). Ako hoćete veliku sigurnost i da se niko ko nema Vaš Certificat ne može ulogovati.**

<http://www.karlrunge.com/x11vnc/ssl.html>

<http://ubuntuforums.org/showthread.php?t=1246978>

Ako imate problema potražite na Internetu

## Siguran prenos Certificata

**Koristite za prenos samo sigurne veze na primer scp, FTP, elektronsku poštu zaštićenu sa GnuPG, Jabber sa OTR...**

## Uvoz SSL VNC Certificata

**Najbolje se pokazalo da se samo kopira sadržaj Certifikata sa Servera i da se unese, to jest importuje, u program koji podržava SSL.**

**Za to najbolje koristite SSVNC, radi odlično.**

**Najčistije da sa komandom cat vidite Certifikat na ekranu i to unesete na primer sa SSVNC u polje gde se importira Certificat.**

**cat certificat**

**SSVNC / Certs / Import Certificate**

**Unesite sadržaj tog Certificata u polje za Paste.**

**Import Certificate / Also save to the 'Accepted Certs' directory**

**Naravno dopustite mu da zapamti Certificat od Servera u**

**~/.vnc/certs/accepted**

**da bi se taj Certificat mogao koristiti za kasnija logovanja.**

Možete samo za probu da li radi da napravite privremeni Certificat, da ga uvezete i vidite da li možete ostvariti vezu.

**x11vnc -ssl TMP**

**Trebate napraviti za x11vnc Certificat i na Serveru**

**Možete to uraditi jednostavno bez da imate svoj CA, ne preporučujem**

[http://www.karlrunge.com/x11vnc/x11vnc\\_opts.html#opt-ssl](http://www.karlrunge.com/x11vnc/x11vnc_opts.html#opt-ssl)

```
x11vnc -ssl SAVE
```

Dobićete podrazumevano ove fajle

```
~/.vnc/certs/server.crt
```

```
~/.vnc/certs/server.pem
```

Bolje je da dodate Vaše [Hostname](#) na imena Certificata da bi se tačno znalo, kao i u [Stunnel](#) primeru

```
x11vnc -ssl SAVE_PROMPT-$(uname -n)
```

Dobićete ove fajle

```
~/.vnc/certs/server-$(uname -n).crt
```

```
~/.vnc/certs/server-$(uname -n).pem
```

**Možete napraviti Certificate Authority, to je mnogo sigurnije i bolje**

[http://www.karlrunge.com/x11vnc/x11vnc\\_opts.html#opt-sslGenCA](http://www.karlrunge.com/x11vnc/x11vnc_opts.html#opt-sslGenCA)

Ovo je default sa RSA 2048 i za vreme od 730 dana

```
x11vnc -sslGenCA
```

Možete imati RSA 4096 i za vreme od 7300 dana

**x11vnc -env REQ\_ARGS='-days 7300 -newkey 4096' -sslGenCA**

Kad Vas pita za Common Name možete navesti umesto Vašeg login imena Vaše [Hostname](#)

```
$(uname -n) x11vnc server CA
```

Dobićete ove fajle

**Javni x11vnc Certificat, koji treba da pošaljete sigurnim putem klijentu, da ga uključi kao Certificat Servera**

**~/.vnc/certs/CA/cacert.pem**

**Vaš privatni x11vnc ključ za Certificate, koristi se da se potpišu Certificati za servera i klijente, čuvajte ga dobro.**

**~/.vnc/certs/CA/private/cakey.pem**

Napravite za Server Certificat i privatni ključ, dodajte na ime Certificata Hostname

[http://www.karlrunge.com/x11vnc/x11vnc\\_opts.html#opt-sslGenCert](http://www.karlrunge.com/x11vnc/x11vnc_opts.html#opt-sslGenCert)

Ovo je default sa RSA 2048 i za vreme od 730 dana

**x11vnc -sslGenCert server**

Možete imati RSA 4096 i za vreme od 7300 dana

**x11vnc -env REQ\_ARGS='-days 7300 -newkey 4096' -sslGenCert server \$(uname -n)**

Dobićete ove fajle

Javni Certificat Servera

**~/.vnc/certs/server-\$(uname -n).crt**

Vaš privatni ključ i javni Certificat Servera

**~/.vnc/certs/server-.\$(uname -n).pem**

Možete sad startati x11vnc na Serveru sa Hostname

```
x11vnc -ssl SAVE
```

```
x11vnc -ssl SAVE-$(uname -n)
```

**Možete napraviti Certificate za Vaše klijente**

**što je još sigurnije, jer je to onda dupla kontrola.**

Ovo je default sa RSA 2048 i za vreme od 730 dana

```
x11vnc -sslGenCert client klijent-Hostname
```

Možete imati RSA 4096 i za vreme od 7300 dana

```
x11vnc -env REQ_ARGS='-days 7300 -newkey 4096' -sslGenCert client client-Hostname
```

Dobićete ove fajle

**Certifikat klijenta, treba da ostane na Serveru**

```
~/.vnc/certs/clients/client-Hostname.crt
```

**Privatni x11vnc ključ za klijenta, koji treba da pošaljete sigurnim putem klijentu, da ga uključi kao svoj Certificat. On nije potreban na Serveru.**

```
~/.vnc/certs/clients/client-Hostname.pem
```

**Treba samo da se nalazi kod klijenta u**

```
~/.vnc/certs
```

Da nađete Hashname od fajli, samo potrebno ako imate više Servera ili klijenata.

[http://www.karlrunge.com/x11vnc/x11vnc\\_opts.html#opt-sslverify](http://www.karlrunge.com/x11vnc/x11vnc_opts.html#opt-sslverify)

```
cd ~/.vnc/certs/clients
```

```
openssl x509 -hash -noout -in klijent-Hostname.crt
```

hash-broj

Možete napraviti hash linkove sa

x11vnc -sslCertInfo HASHON

Možete izbrisati hash linkove sa

x11vnc -sslCertInfo HASHOFF

**Startajte x11vnc Server sa Hostname i sa podrškom za Certificate od klijenata**

**Najbolje da koristite -sslverify sa Certificate Authority, dobro radi**

**x11vnc -rc ~/.x11vncrc-ssl -ssl SAVE-\$(uname -n) -sslverify CA >> ~/.x11vnc-ssl.log 2>&1 &**

## SSL Tunnel viewers

<http://www.karlrunge.com/x11vnc/faq.html#faq-ssl-tunnel-viewers>

Da bi ovi SSL viewer mogli da rade mora da bude podignut  
x11vnc sa SSL podrškom za Certificate Servera i klijenata.

ss\_vncviewer i SSL Tunnel

Koristi TigerVNC, radi odlično.

/home/bin/vncviewer-ss-ssl

SSVNC i SSL Tunnel

Koristi svoj ugrađeni viewer, radi odlično.

Ove metode za startanje x11vnc Servera tako sigurne i ne uspevaju uvek,  
**najbolje je da se kompletni CA proveri.**

Ako imate jednog klijenta, navedite njegov Certificat

```
x11vnc -ssl SAVE-$(uname -n) -sslverify ~/.vnc/certs/clients/client-Hostname.crt
```

Ako imate više klijenata, može biti onda direktorijum sa hash linkovima

```
x11vnc -ssl SAVE-$(uname -n) -sslverify ~/.vnc/certs/clients/HASH
```

## **Da vidite Vaše Certificate**

[http://www.karlrunge.com/x11vnc/x11vnc\\_opts.html#opt-sslCertInfo](http://www.karlrunge.com/x11vnc/x11vnc_opts.html#opt-sslCertInfo)

Kratka lista samo koje Certificate imate

**x11vnc -sslCertInfo list**

Dugačka lista Certificata sa svim podatcima

**x11vnc -sslCertInfo all**

## **Možete opozvati Certificate klijentata**

[http://www.karlrunge.com/x11vnc/x11vnc\\_opts.html#opt-ssICRL](http://www.karlrunge.com/x11vnc/x11vnc_opts.html#opt-ssICRL)

## Povezivanje preko X protokola

Ako imate više kompjutera a jednu tastaturu i jednog miša

Preko SSH protokola na udaljeni X

VNC protokol, Virtual Network Computing

NX protokol

Linux Terminal Server Project

RDP protokol, Remote Desktop Protokol

GUI za razne protokole

Ostala rešenja za povezivanje preko X protokola

Na početak

## **NX protokol**

Pogledajte uputstva na

[https://secure.wikimedia.org/wikipedia/en/wiki/NX\\_technology](https://secure.wikimedia.org/wikipedia/en/wiki/NX_technology)

<http://www.nomachine.com/configuration.php>

<http://www.gentoo-wiki.info/FreeNX>

<https://help.ubuntu.com/community/FreeNX>

<http://www.linux.com/news/enterprise/networking/8251-faster-remote-desktop-connections-with-freenx>

Da vidite šta ima

Za [BSD](#)

```
find /usr/ports/* | grep freenx
```

Za [GNU/Linux](#)

```
eix freenx
```

```
eix -S freenx
```

```
eix -S nx
```

## **FreeNX**

NX Server, potpuno slobodna verzija

<http://freenx.berlios.de>

<https://launchpad.net/freenx>

<https://launchpad.net/freenx-server>

<https://launchpad.net/~freenx-team>

Za [BSD](#)

```
portmaster -n net/freenx
```

### Za GNU/Linux

Da se koristi nxclient stavite u

```
/etc/paludis/etc.use
```

```
...  
net-misc/nxserver-freenx nxclient  
...
```

```
emerge -a net-misc/nxserver-freenx
```

Da bi startali NX Server

```
/etc/init.d/nxserver start
```

Da bi uvek startan pri podizanju sistema

```
rc-update add nxserver default
```

### **NX Free Edition**

Free edition NX server from NoMachine

Slobodna verzija, samo 2 korisnika istovremeno.

<http://www.nomachine.com>

### Za GNU/Linux

```
emerge -a net-misc/nxserver-freeedition
```

### **Neatx**

Google implementation of NX server

<https://code.google.com/p/neatx/>

Za [GNU/Linux](#)

```
emerge -a neatx
```

## Eagleeye

GTK FreeNX client

<https://code.launchpad.net/~freenx-team/freenx-server/eagleeye>

Za [GNU/Linux](#)

```
emerge -a net-misc/eagleeye
```

## Qt FreeNX

Qt FreeNX klient

<http://developer.berlios.de/projects/freenx/>

Za [GNU/Linux](#)

```
emerge -a net-misc/qtnx
```

## Linux Terminal Server Project

<http://ltsp.org/>

<http://sourceforge.net/apps/mediawiki/ltsp/index.php>

[http://sourceforge.net/apps/mediawiki/ltsp/index.php?title=Ltsp\\_Documentation](http://sourceforge.net/apps/mediawiki/ltsp/index.php?title=Ltsp_Documentation)

<http://www.gentoo.org/doc/en/ltsp.xml>

<http://en.gentoo-wiki.com/wiki/LTSP>

<http://www.ns-linux.org/Uputstva/Gentoo/ltsp/>

<http://www.gentoo.org/doc/en/ldap-howto.xml>

[http://www.yolinux.com/TUTORIALS/LDAP\\_Authentication.html](http://www.yolinux.com/TUTORIALS/LDAP_Authentication.html)

<http://etherboot.org/wiki/index.php>

Dobro je za škole i ako imate kompjutere bez Harddiskova. Mogu biti stari kompjuteri i samo jedan jači Server koji opslužuje sve ostale kompjutere.

Takođe možete za škole koristiti i [iTALC](#).

## **RDP protokol, Remote Desktop Protokol**

[https://secure.wikimedia.org/wikipedia/en/wiki/Remote\\_desktop\\_software](https://secure.wikimedia.org/wikipedia/en/wiki/Remote_desktop_software)

<http://ns-linux.org/Uputstva/Opste/kako-napraviti-remote-desktop-konekciju-ssh-tunelom-sa-linux-racunala-na-udaljeni-windows-xp-2003-pc>

### **rdesktop**

A [Remote Desktop Protocol](#) Client

<http://www.rdesktop.org/>

Za [BSD](#)

```
portmaster -n net/rdesktop
```

Za [GNU/Linux](#)

```
emerge -a rdesktop
```

### **grdesktop**

Gtk2 frontend for [rdesktop](#)

<http://www.nongnu.org/grdesktop/>

Za [BSD](#)

```
portmaster -n net/grdesktop
```

Za [GNU/Linux](#)

```
emerge -a grdesktop
```

## **jrdesktop**

Java Remote Desktop software for viewing and / or controlling a distance PC

Java [GUI](#) za [RDP](#), bolje koristiti [grdesktop](#).

<http://jrdesktop.sourceforge.net/>

Za [BSD](#)

```
portmaster -n net/jrdesktop
```

Za [GNU/Linux](#)

```
emerge -a jrdesktop
```

## **GUI za razne protokole**

### **Remmina**

A GTK+ [RDP](#), [VNC](#), XDMCP and [SSH](#) client

Is a remote desktop client written in GTK+, aiming to be useful for system administrators and travellers, who need to work with lots of remote computers in front of either large monitors or tiny netbooks. Remmina supports multiple network protocols in an integrated and consistant user interface.

<http://sourceforge.net/projects/remmina/>

Za [BSD](#)

```
portmaster -n net/remmina net/remmina-plugins
```

Za [GNU/Linux](#)

```
emerge -a remmina remmina-plugins
```

## Window Switch

Is a client server tool to start and control virtual desktops

Može da koristi [VNC](#), [xpra](#), [NX](#), [RDP](#), [SSH](#)

<http://winswitch.org/>

Za [GNU/Linux](#)

```
emerge -a winswitch
```

Na stranici ima ebulda za [Window Switch](#) i [xpra](#)

## Xrdp

An [Free Software remote desktop protocol](#) (rdp) server

Koristi [rdesktop](#), umesto [smopu!M](#) Servera.

Daje korisniku normalni X Window Desktop a ne [smopu!M](#) Desktop.

Može da koristi [VNC](#) ,[RDP](#)

<http://xrdp.sourceforge.net/>

<http://en.gentoo-wiki.com/wiki/Xrdp>

Za [BSD](#)

```
portmaster -n net/xrdp
```

Za [GNU/Linux](#)

```
emerge -a xrdp
```

## KRDC

[KDE remote desktop connection](#) ([RDP](#) and [VNC](#)) client

<http://uwolfer.fwo.ch/blog/>

Za [GNU/Linux](#)

```
emerge -a krdc
```

## Ostala rešenja za povezivanje preko X protokola

### **xpra, X Persistent Remote Apps**

Gives you persistent remote applications for X. So basically it's screen for remote X apps.

Omogućava da startate na Serveru programe i da samo napustite sesiju, i da ih ponovo uključite, slično kao što možete imati za [konzolu sa specijalnim programima za umnožavanje](#).

Ako želite na Serveru da koristite kompletno okruženje možete za to uzeti [VNC](#).

<http://xpra.devloop.org.uk/>

<https://code.google.com/p/partiwm/wiki/xpra>

<https://code.google.com/p/partiwm/source/browse/README.xpra>

Za [BSD](#)

```
portmaster -n x11/xpra
```

Za [GNU/Linux](#)

Deo [partiwm](#) Window Manager-a i [Window Switch](#)-a

```
man xpra
```

Na serveru ako koristite više portove za [SSH](#)

```
xpra start :0 --bind-tcp=Viši-port
```

Na klijentu ako koristite više portove za [SSH](#) na primer

```
xpra attach --ssh="ssh -i ~/.ssh/privat_dsa -p Viši-port:server:0"
```

## **Hamachi**

The free version may be used for a limited 14-day evaluation period in a commercial environment.

Na stranici daju da se skine msi fajla za smopu!M

Do 16 kompjutera može da se konektuje

<http://hamachi.cc>

<https://secure.logmein.com/products/hamachi2/>

Za BSD

portmaster -n security/hamachi

Za GNU/Linux

emerge -a hamachi

## **gHamachi**

GUI za Hamachi

<http://tools.harvie.cz/hamachi/>

<http://linux.softpedia.com/progDownload/gHamachi-Download-30358.html>

<http://ruined.wikidot.com/howtoprivatevpn>

...

Instališe se ručno.

## **LogMeIn**

GUI za OpenVPN

<https://secure.logmein.com/US/products/free/>

Morate se registrovati na stranici da bi mogli koristiti ovaj servis.

## TeamViewer

Možete ga koristiti da pomognete smopu!M zavisnicima.

Uradite sve da pređu na sigurniji BSD ili GNU/Linux, ili koristite ovo samo kao prva pomoć dok se ne možete povezati preko sigurnijih metoda.

Ulogujete se preko njihove adrese i ID koji se generiše na drugi kompjuter, od kojeg morate znati iste podatke.

Najbolje navedite smopu!M zavisnike da koriste bar za te važne informacije za Instant Messaging otvoreni Jabber protokol i OTR, a ne MSN.

<http://www.teamviewer.com/>

Instališe se ručno. Radi dobro sa Emulatorima za operativne sisteme.

<http://www.administrator.de/index.php?content=111713>

<http://www.linuxine.com/story/how-use-teamviewer-share-files-and-remotely-control-another-computer>

Napravite direktorijum i uđite u njega

```
mkdir -p "/paketi/Operativni_sistemi/Windows/TeamViewer/Source"  
cd "/paketi/Operativni_sistemi/Windows/TeamViewer/Source"
```

Skinite za BSD i GNU/Linux

```
wget http://www.teamviewer.com/download/teamviewer_linux.tar.gz
```

Linkujte sa

```
In -s TeamViewer_Setup.exe ..../TeamViewer.exe
```

Ili skinite za smopu!M, svejedno to je samo zapakovano sa starijom verzijom Wine

```
wget http://www.teamviewer.com/download/TeamViewer_Setup.exe
```

Možete ga startati i preko [emulatora za operativne sisteme](#), pokrenite ga kao normalni program.

### Povezivanje preko X protokola

[Ako imate više kompjutera a jednu tastaturu i jednog miša](#)

[Preko SSH protokola na udaljeni X](#)

[VNC protokol, Virtual Network Computing](#)

[NX protokol](#)

[Linux Terminal Server Project](#)

[RDP protokol, Remote Desktop Protokol](#)

[GUI za razne protokole](#)

[Ostala rešenja za povezivanje preko X protokola](#)

[Na početak](#)

## **Kontrolisanje tastature i miša**

Ovakve alate koriste Crackeri da Vam nanesu štetu.

### **Xnee**

Program suite to record, replay and distribute user actions.

Ovaj program je baš za Hacker-e da Vas kontrolišu šta pišete i šta radite sa mišem.

Ali možete pisati razne dobre skriptice koje izvršavaju ono što ste radili i može Vam olakšati neke stvari.

<http://www.sandklef.com/xnee>

Za [BSD](#)

```
portmaster -n x11/xnee
```

Za [GNU/Linux](#)

```
emerge -a xnee
```

Treba da imate izvršne fajle

```
cnee
```

## PyKeylogger

Is a [Free Software](#) keylogger

[http://sourceforge.net/apps/mediawiki/pykeylogger/index.php?title=Main\\_Page](http://sourceforge.net/apps/mediawiki/pykeylogger/index.php?title=Main_Page)

[Instališe se ručno.](#)

## logkeys

Linux keylogger

<https://code.google.com/p/logkeys/>

[Instališe se ručno.](#)

<http://askubuntu.com/questions/14312/how-to-run-logkeys>

## LKL

Is a userspace keylogger that runs under Linux on the x86 arch

<http://sourceforge.net/projects/lkl/>

[Instališe se ručno.](#)

[Na početak](#)

## Centralno održavanje više kompjutera

<http://www.gentoo.org/news/en/gmn/20080930-newsletter.xml>

<http://www.gentoo.org/news/en/gmn/20081130-newsletter.xml>

<http://www.linux.com/feature/151340>

<http://tentakel.biskalar.de/similar/>

Na mnogim stranicama ima linkova za još programa. Obično to piše kao *Similar programs*.

Pogledajte [SSH i prevodjenje](#) i [Možete koristiti specijalne programe za umnožavanje](#).

Koristim najviše [Tar](#), [dd](#) za većinu lokalnih osiguranja.

Preko Interneta i u lokalu koristim najviše [Rsync](#) za na primer izjednačavanje kompjutera.

## Webmin

Webmin is a web-based interface for system administration for Unix. Using any browser that supports tables and forms, you can setup user accounts, Apache, DNS, file sharing and so on.

Webmin consists of a simple web server, and a number of CGI programs which directly update system files like /etc/inetd.conf and /etc/master.passwd.

<http://www.webmin.com/webmin/>

Za [BSD](#)

```
portmaster -n sysutils/webmin
```

Za [GNU/Linux](#)

```
emerge -a webmin
```

Za [BSD](#)

[/etc/rc.conf](#)

```
webmin_enable="YES"
```

```
/usr/local/etc/rc.d/webmin start
```

Za [GNU/Linux](#)

```
rc-update add webmin default
```

Konfigurišite sa

```
/usr/local/lib/webmin/setup.sh
```

Treba da imate jednog korisnika na primer webmin, ili [Korisnik za Internet protokole](#).

## ClusterSSH

Controls a number of [Xterm](#) windows via a single graphical console window to allow commands to be interactively run on multiple servers over an [SSH](#) connection.

<http://clusterssh.sourceforge.net>

Za [BSD](#)

```
portmaster -n security/clusterssh
```

Za [GNU/Linux](#)

```
emerge -a clusterssh
```

<http://www.linux.com/news/featured-blogs/193-original-linux-tutorials/413853-managing-multiple-linux-servers-with-clusterssh>

<http://www.edwigit.name/2011/11/administration-clusterssh/>

## PSSH, Parallel SSH Tools

Provides parallel versions of [OpenSSH](#) and related tools. Included are pssh, pscp, prsync, pnuke, and pslurp. The project includes psshlib which can be used within custom applications.

Ova stranica se više ne održava

<http://www.theether.org/pssh>

Nastavak razvoja coda

<http://code.google.com/p/parallel-ssh>

Za [BSD](#)

```
portmaster -n security/pssh
```

## Za [GNU/Linux](#)

```
emerge -a pssh
```

## Tentakel

Is a program for executing the same command on many hosts in parallel using various remote methods. It can make use of several sets of hosts that are defined in a configuration file as groups.

<http://tentakel.biskalar.de>

## Za [BSD](#)

```
portmaster -n sysutils/tentakel
```

## Za [GNU/Linux](#)

```
emerge -a tentakel
```

## shmux

Program for executing the same command on many hosts in parallel. For each target, a child process is spawned by shmux, and a shell on the target obtained one of the supported methods: rsh, [SSH](#), or sh. The output produced by the children is received by shmux and either (optionally) output in turn to the user using an easy to read format, or written to files for later processing making it well suited for use in scripts.

<http://web.taranis.org/shmux/>

## Za [BSD](#)

```
portmaster -n net/shmux
```

## Za [GNU/Linux](#)

```
emerge -a shmux
```

## Pdsh, Parallel Distributed Shell

A high-performance, parallel remote shell utility

It has built-in, thread-safe clients for Berkeley and Kerberos V4 rsh and can call [SSH](#) externally (though with reduced performance). [Pdsh](#) uses a "sliding window" parallel algorithm to conserve socket resources on the initiating node and to allow progress to continue while timeouts occur on some connections.

<https://code.google.com/p/pdsh/>

<https://computing.llnl.gov/linux/pdsh.html>

<http://sourceforge.net/projects/pdsh/>

Ima dobrih utility za rad sa [Pdsh](#)-om

<https://computing.llnl.gov/linux/downloads.html>

Za [BSD](#)

```
portmaster -n sysutils/pdsh
```

Za [GNU/Linux](#)

```
emerge -a pdsh
```

## Mussh

Is a shell script that allows you to execute a command or script over [SSH](#) on multiple hosts with one command. When possible mussh will use ssh-agent and RSA/DSA keys to minimize the need to enter your password more than once.

<http://sourceforge.net/projects/mussh/>

Za [BSD](#)

```
portmaster -n security/mussh
```

## Polysh

Is a tool to aggregate several remote shells into one. It is used to launch an interactive remote shell on many machines at once.

<http://guichaz.free.fr/polysh/>

Za [GNU/Linux](#)

```
emerge -a polysh
```

## KontrolPack

Remote shell command executor and LAN manager

<http://www.kontrolpack.com/>

Za [GNU/Linux](#)

```
emerge -a kontrolpack
```

## Unison

Two-way cross-platform file synchronizer

<http://www.cis.upenn.edu/~bcpierce/unison/>

Za [BSD](#)

```
portmaster -n net/unison-verzija
```

Za [GNU/Linux](#)

```
emerge -a unison
```

## Duplicity

Backs directories by producing encrypted tar-format volumes and uploading them to a remote or local file server. Because duplicity uses librsync, the incremental archives are space efficient and only record the parts of files that have changed since the last backup. Because [Duplicity](#) uses [GnuPG](#) to encrypt and/or sign these archives, they will be safe from spying and/or modification by the server.

Može koristiti [SSH](#), [Rsync](#)...

<http://www.nongnu.org/duplicity/>

Za [BSD](#)

```
portmaster -n sysutils/duplicity-verzija
```

Za [GNU/Linux](#)

```
emerge -a app-backup/duplicity
```

## **MCollective, Marionette Collective**

Framework to build server orchestration or parallel job execution systems.

<http://docs.puppetlabs.com/mcollective/>

Za [BSD](#)

```
portmaster -n www/sitecopy
```

Za [GNU/Linux](#)

```
emerge -a mcollective
```

## **Gigolo**

Is a frontend to easily manage connections to local and remote filesystems using GIO/GVfs. It allows you to quickly connect/mount a remote filesystem and manage bookmarks of such.

It is part of the Xfce Goodies project and the Subversion repository is hosted on the Xfce servers though it does not have any hard Xfce dependencies and can be used on other desktop environments as well. The only hard dependency is GTK2.

<http://www.uvena.de/gigolo/>

Za [BSD](#)

[Napravio sam FreeBSD Port](#), poslao sam ga na [RedPorts](#) 19.07.2012, , kao [PR](#) 20.07.2012,

Za [GNU/Linux](#)

```
emerge -a gigolo
```

[Centralno održavanje više kompjutera](#)

[ClusterSSH](#)

[PSSH, Parallel SSH Tools](#)

[Tentakel](#)

[shmux](#)

[Mussh](#)

[Pdsh, Parallel Distributed Shell](#)

[Polysh](#)

[KontrolPack](#)

[Unison](#)

[Duplicity](#)

[MCollective, Marionette Collective](#)

[Na početak](#)

## **Samba protokol**

Da vidite šta ima

Za [BSD](#)

```
find /usr/ports/* | grep samba
```

Za [GNU/Linux](#)

```
eix samba
```

```
eix -S samba
```

<http://www.techrepublic.com/blog/10things/10-ways-to-make-your-samba-life-easier/1461>

<http://linuxpoison.blogspot.com/2008/07/quick-and-simple-samba-configuration.html>

Možete koristiti [SMB for Fuse](#) da mountujete Samba share

## **Samba**

Samba Server component

The Samba suite is a set of programs which run under the [FreeBSD](#) operating system. These programs deliver most of the important functionality of a Microsoft Lan Manager server. That is, they support remote access to [FreeBSD](#) filesystem and [FreeBSD](#) printers from Lan Manager compatible clients. In practical terms, this means that such clients can connect to and use [FreeBSD](#) filesystem as if it was a local disk drive, or [FreeBSD](#) printers as if they were local printers.

Some of the most popular Lan Manager compatible clients include Lan Manager itself, Windows for Workgroups, OS/2 and Windows NT.

Verovatno već imate instalisano

<http://www.samba.org/>

Za [BSD](#)

portmaster -n net/samba-verzija

Za [GNU/Linux](#)

emerge -a samba

Da podignite

/etc/init.d/samba start

Da se stalno podiže pri startanju sistema

rc-update add samba default

Kome treba da se poveže sa [smopu!M](#) PC-om, neka potraži na Internetu

smb.conf BSD

smb.conf Linux

Pogledajte

<http://www.elitesecurity.org/t362658-Samba-Pitanje-oko-konfiguracije-etc-smb-conf>

Meni su ti svi Port-ovi isključeni, to jest zabranjeni u mom zaštitnom zidu, da ne bih imao napade koji su upereni protiv [smopu!M](#) korisnika.

A lako će ih otvoriti ako mi zatrebaju.

**SambaScanner**

A tool to search a whole [Samba](#) network for files

<http://www.johannes-bauer.com/software/sambascanner/>

Za [GNU/Linux](#)

```
emerge -a sambascanner
```

[Na početak](#)

## **PPTP Protokol, Microsoft Point-to-Point Tunneling Protocol**

Je zatvoreni način na koji se može koristiti [Virtual Private Network](#).

### **Poptop**

Linux Point-to-Point Tunnelling Protocol Server

<http://www.poptop.org/>

```
emerge -a net-dialup/pptpd
```

### **PPTP Client**

This is a port of the "pptp-linux" PPTP client. It can establish a PPP connection with an NT server, tunneled through a PPTP link over the Internet. In effect, it makes the client machine behave as if it were on the same LAN as the server.

<http://pptpclient.sourceforge.net/>

Za [BSD](#)

```
portmaster -n net/pptpclient
```

Za [GNU/Linux](#)

```
emerge -a net-dialup/pptpclient
```

[Na početak](#)

## **Kombinovana rešenja za razne protokole**

### **NetworkManager**

Network configuration and management in an easy way. Desktop environment independent.

<http://projects.gnome.org/NetworkManager/>

```
emerge -a networkmanager
```

Dodatke možete vidite sa

```
eix networkmanager
```

```
eix -S networkmanager
```

### **Smartcard**

Da vidite šta ima

```
eix -S smart
```

Pogledajte [RFID](#).

Blog

<http://ludovicrousseau.blogspot.com/>

### **PCSC-Lite**

PC/SC Architecture smartcard middleware library

<http://pcsclite.alioth.debian.org/>

emerge -a pcsc-lite

## OpenCT

Library for accessing smart card terminals

<http://www.opensc-project.org/openct/>

emerge -a openct

## OpenCT Phoenix/SM driver

A basic driver for the [OpenCT](#) framework that provides a support for Phoenix / SmartMouse smartcard readers.

<http://sourceforge.net/projects/openct-phoenix/>

[Instališe se ručno.](#)

## OpenSC

Libraries and applications to access smartcards.

<http://www.opensc-project.org/opensc>

emerge -a opensc

Koji sve programi mogu koristiti [OpenSC](#)

<http://www.opensc-project.org/opensc/wiki/ApplicationSupport>

## pcsc-tools

These tools are used to test a PC/SC driver, card or reader or send commands in a friendly environment (text or graphical user interface).

<http://ludovic.rousseau.free.fr/softwares/pcsc-tools/>

emerge -a pcsc-tools

Pogledajte veoma veliku listu karata i ATR vrednosti

[http://ludovic.rousseau.free.fr/softwares/pcsc-tools/smardcard\\_list.txt](http://ludovic.rousseau.free.fr/softwares/pcsc-tools/smardcard_list.txt)

## **CCID**

CCID [Free Software](#) driver

Provides the source code for a generic USB CCID (Chip/Smart Card Interface Devices) driver and ICCD (Integrated Circuit(s) Card Devices).

<http://pcsclite.alioth.debian.org/ccid.html>

emerge -a ccid

## **pyscard**

Is a python module adding smart cards support to python.

<http://pyscard.sourceforge.net/>

emerge -a pyscard

## **pssi**

Python Simple Smartcard Interpreter

Python script that provides an abstract layer for smartcard reading. Thanks to it, it is possible to read a smartcard by simply adding its structure in the form of a plugin, without taking care of the communication layer. The tool comes with several plugins, namely SIM, EMV, Navigo and Belgian eID.

<https://code.google.com/p/pssi/>

emerge -a pssi

## **Freesteel**

Freesteel project contains pyfreesteel (Python) and jfreesteel (Java) source repositories.

<http://gitorious.org/freesteel>

Instališe se ručno.

Možete skinuti sa ovim skriptama

/home/bin/git/git-FreesteelJava

/home/bin/git/git-FreesteelPython

[http://blog.goranrakic.com/archives/2011/01/gui\\_za\\_citac\\_licne\\_karte\\_provirivanje.html](http://blog.goranrakic.com/archives/2011/01/gui_za_citac_licne_karte_provirivanje.html)

Na početak

Datum promene

25.11.2012