HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Trinux distribucija

CCERT-PUBDOC-2002-12-10

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

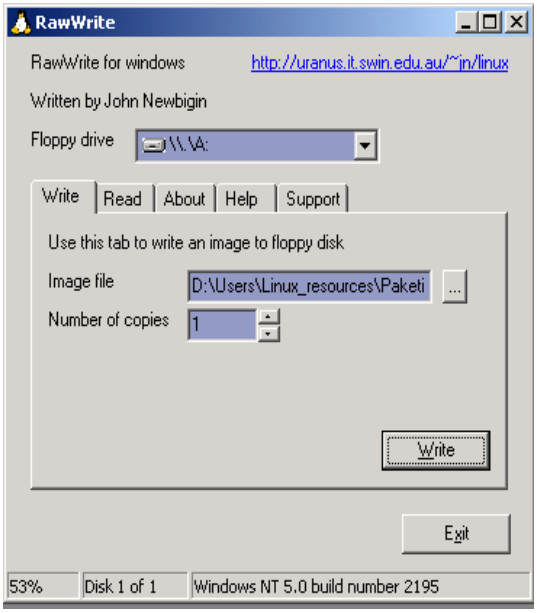
Trinux je Linux distribucija bazirana na RAM disk načinu rada, koja sadrži sve trenutno najpopularnije *open source* sigurnosne alate. RAM disk je način rada u kojemu se dio radne memorije sustava (RAM) koristi kao zamjena za prostor na tvrdom disku. Drugim riječima, područje radne memorije preuzima ulogu tvrdog diska na koji se spremaju i sa kojeg se čitaju svi podaci.
Trinux sustav može se podizati (eng. *boot*) ili sa diskete ili sa CD-ROM- a, a raspoložive programske pakete moguće je po potrebi učitati sa HTTP ili FTP poslužitelja, FAT/NTFS/ISO datotečnog sustava ili sa drugih disketa. Distribucija sadrži mnoštvo sigurnosnih alata namijenjenih pregledavanju mrežnih portova (eng. *port scanning*), analiziranju i praćenju mrežnog prometa (eng. *sniffing*), lažiranju paketa (eng. *spoofing*), forenzičkoj analizi (eng. *forensics*) i sl., što je čini posebno korisnom sistem administratorima te svima onima koji se bave područjem računalne sigurnosti. S obzirom na karakteristike i namjenu pojedinih alata sadržanih u distribuciji, ista bi mogla biti interesantna i neovlaštenim korisnicima prilikom provođenja njihovih malicioznih aktivnosti.
Osnovna prednost Trinux distribucije je jednostavnost korištenja velikog broja Linux *open source* sigurnosnih alata, bez potrebe za instalacijom Linux operacijskog sustava i pojedinih paketa.

2. Instalacija

Instalacija Trinux distribucije bazira se na izradi odgovarajućih disketa ili CDROM medija putem kojih će se omogućiti podizanje sustava. Ovisno o načinu na koji se odgovarajući sigurnosni alati žele učitavati (putem mreže, datotečnog sustava ili sl.) potrebno je dobaviti jedan od sljedećih paketa:

- `trinux-0.80rc2-ide.img` – distribucija s Linux jezgrom koja sadrži podršku za IDE tvrde diskove, CD-ROM uređaje te FAT, NTFS i minix datotečne sustave. Ovaj paket koristi se u situacijama kada se paketi žele instalirati sa tvrdog diska ili CD-ROM uređaja.
- `trinux-0.80rc2-net.img` – distribucija s Linux jezgrom koja sadrži podršku za popularnije Ethernet mrežne kartice. U ovom slučaju učitavanje programskih alata moguće je ili putem HTTP ili FTP poslužitelja, budući da u jezgru nije integrirana podrška za IDE uređaje.
- `trinux-0.80rc2-pcmcia.img` – distribucija s najmanjom Linux jezgrom, bez ugrađene podrške za ISA/PCI Ethernet mrežne kartice ili IDE uređaje. Jezgra uključuje module koji podržavaju 3Com, Xircom te još neke PCMCIA mrežne kartice čime se omogućuje učitavanje pojedinih paketa putem mreže. Lista podržanih kartica dostupna je na adresi http://pcmcia-cs.sourceforge.net/ftp/SUPPORTED.CARDS .

Budući da su svi Trinux paketi dostupni kao *image* datoteke, nije ih moguće kopirati standardnim postupcima. Potrebno je koristiti posebno prilagođene alate koji će omogućiti snimanje *image* zapisa na disketu. Primjer takvog alata je `rawwrite` program koji je dostupan za DOS i Windows operacijske sustave. Na slici (Slika 1) prikazan je izgled `rawwrite` programa za MS Windows operacijske sustave putem kojeg je `trinux-0.80rc2-ide.img` datoteka zapisana na disketu.



Slika 1 - `Rawwrite` program za windows operacisjki sustav

Nakon što je na opisani način kreirana *boot* disketa moguće je podignuti Trinux operacijski sustav (nakon što se u BIOS-u računala podesi prikladna *boot* sekvenca; potrebno je disketnu jedinicu staviti kao prvi uređaj s kojeg se podiže sustav). Instalacija paketa i način njihove instalacije opisan je u nastavku dokumenta.

Budući da se kod Trinux operacijskog sustava sve konfiguracijske datoteke, podaci te učitani programski paketi nalaze u radnoj memoriji, isti će nakon gašenja sustava biti nepovratno izgubljeni. Podaci koji su trajno zapisani na disketu prilikom njenog kreiranja uključuju jezgru operacijskog sustave te neke osnovne pakete i konfiguracijske datoteke potrebne za podizanje sustava. Sve ostale datoteke i paketi, koje se naknadno kreiraju kao posljedica korištenja sustava, nalaziti će se u radnoj memoriji i neće biti zapisani na disketu.

Upravo iz tog razloga postoji posebna grupa naredbi kojima je moguće naknadne promjene u konfiguraciji trajno zapisati na disketu, kako bi se kao takve uzele u obzir prilikom sljedećeg podizanja sustava. Primjer takve naredbe je `savecfg` naredba kojom se sadržaj `/etc/tux` direktorija zapisuje na disketu. Postoje još i naredbe `savehome` i `gethome` kojima se `/home` direktorij korisnika može učitati ili pohraniti na udaljeno računalo putem FTP ili HTTP protokola. Na ovaj način korisniku je omogućeno očuvanje sadržaja *home* direktorija, čime se dodatno pokušavaju kompenzirati nedostatci RAM disk načina rada.

3. Učitavanje paketa

Trinux distribucija podržava nekoliko načina učitavanja raspoloživih programskih paketa. To su:

- putem mreže
- putem tvrdog diska ili CDROM uređaja
- putem dodatnih disketa

U nastavku će ukratko biti opisana svaka od podržanih metoda učitavanja paketa.

3.1. Učitavanje paketa putem mreže

Učitavanje programskih paketa putem mreže svakako je najpraktičnije i najjednostavnije rješenje, pogotovo u mrežnim okolinama s većom propusnošću. Treba još jednom napomenuti da je ovaj način učitavanja paketa podržan kod `trinux-0.80rc2-net.img` i `trinux-0.80rc2-pcmcia.img` distribucija.

Podešavanje mreže u oba slučaja može se obaviti na dva načina, ili statičkim dodjeljivanjem IP adrese ili putem DHCP protokola. U inicijalnoj konfiguraciji koristi se DHCP protokol, budući da se isti smatra jednostavnijim za podešavanje. Ukoliko je u sklopu računalne mreže, na kojoj se želi koristiti Trinux

sustav, instaliran DHCP poslužitelj, preporučuje se korištenje istoga s obzirom na jednostavnost postupka. Ukoliko to nije slučaj, potrebno je koristiti statičke IP adrese.
Ukoliko se želi koristiti statičko dodjeljivanje IP adrese potrebno je prethodno onemogućiti DHCP način podešavanja mreže. Isti se onemogućuje kopiranjem `/etc/tux/options/dhcp` datoteke u `/etc/tux/options/disabled` direktorij (isti učinak moguće je postići brisanjem iste datoteke).
Nakon onemogućavanja DHCP-a potrebno je u `/etc/tux/config/` direktoriju dodati sljedeće datoteke koje će omogućiti statičko podešavanje mrežnog sučelja:

- `dns` – IP adresa DNS poslužitelja koji se želi koristiti za prevođenje FQDN imena u IP adrese;
- `gateway` – IP adresa mrežnog usmjerivača;
- `eth0` – statička IP adresa računala, zajedno s mrežnom maskom računalne mreže;

Nakon definiranja istih ne smije se zaboraviti njihovo pohranjivanje `savecfg` naredbom, budući da u suprotnom definirane promjene neće biti uzete u obzir prilikom sljedećeg podizanja sustava.
Učitavanje dostupnih Trinux paketa moguće je obaviti putem HTTP ili FTP poslužitelja. Lista dostupnih *mirror* poslužitelja s kojih je moguće instalirati pakete nalazi se na URL adresi http://trinux.sourceforge.net/mirrors.html.
Inicijalna lista paketa koji će biti učitani prilikom podizanja sustava definirana je `/etc/tux/config/pkglist` datotekom. Svi paketi navedeni u istoj učitati će se prilikom svakog podizanja sustava, sa lokacija definiranih `/etc/tux/config/server` datotekom.
Ostale dostupne pakete moguće je po potrebi naknadno instalirati `getpkg` naredbom. Sintaksa naredbe je:

```
# getpkg ime_paketa
```

Npr.

```
# getpkg nmap
```

naredba rezultirati će instalacijom `nmap` programa za pregledavanje mrežnih portova. Na sličan način moguće je učitati i sve ostale pakete Trinux distribucije.

3.2. Učitavanje paketa sa tvrdog diska ili CD-ROM uređaja

Učitavanje paketa s tvrdog diska najbrža je metoda od svih podržanih. U ovom slučaju potrebno je koristiti `trinux-0.80rc2-ide.img` distribuciju, budući da jedino ona podržava učitavanje paketa s tvrdog diska ili CD-ROM uređaja.
Za uspješno učitavanje paketa na ovaj način potrebno je u korijenu (eng. *root*) datotečnog sustava (C:, D:, /, ...) kreirati `trinux` direktorij sa svim paketima koji se žele učitavati na ovaj način. Učitavanje paketa obaviti će se tijekom podizanja sustava nakon što jezgra (eng. *kernel*) prepozna format datotečnog sustava te `trinux` direktorij sa potrebnim paketima.
Trinux operacijski sustav podržava sljedeće datotečne sustave s kojih je moguće učitavati pakete:

- FAT 16/32
- ext2
- NTFS
- minix
- ISO9660

Prilikom testiranja ove metode učitavanja paketa uočeni su određeni problemi koje bi trebalo spomenuti.
Naime, za učitavanje paketa s tvrdog diska potrebno je na disketi posjedovati `ide.tgz` paket, u kojem je sadržana podrška za IDE uređaje (spomenuti paket ne dolazi kao dio `trinux-0.80rc2-ide.img` distribucije).
Dodatni problem je u tome što na inicijalnoj *boot* disketi ne postoji dovoljno mjesta za kopiranje spomenutog paketa te je stoga potrebno ukloniti neke druge datoteke kako bi se napravilo mjesta za neophodni `ide.tgz` paket. Uklanjanje paketa treba obaviti pažljivo budući da brisanje pogrešnih datoteka može onemogućiti podizanje sustava.
U svrhu testiranja uklonjen je s diskete `dhcpcd.tgz` paket koji omogućuje podešavanje mrežnih parametara putem DHCP protokola. Njegovim uklanjanjem onemogućeno je korištenje DHCP protokola te je stoga u ovom slučaju potrebno statički podesiti mrežne parametre na način kako je to opisano u prethodnom poglavlju (3.1).

Ukoliko se paketi žele učitavati s NTFS datotečnog sustava potrebno je na *boot* disketu dodatno kopirati `ntfs.o` modul jezgre koji će omogućiti korištenje NTFS sustava.

3.3. Učitavanje paketa sa disketa

Učitavanje paketa s dodatnih disketa najsporiji je postupak od svih podržanih te se stoga ne preporučuje osim ukoliko ne postoji druga mogućnost. U ovom slučaju potrebno je na nekoliko dodatnih disketa (ovisno o broju paketa) kopirati željene pakete kako bi se na taj način omogućilo njihovo učitavanje.
Ukoliko se prilikom podizanja sustava ne može kontaktirati niti jedan od navedenih *mirror* poslužitelja, a ne postoji `trinux` direktorij s raspoloživim paketima, biti će ponuđena opcija učitavanja paketa putem disketa.

4. Paketi

Trinux distribucija sadrži prilično velik broj sigurnosnih alata koji se mogu po potrebi učitati i koristiti. Radi se o gotovo svim popularnijim *open source* sigurnosnim alatima koji su dostupni za Linux operacijske sustave. U nastavku je dana lista dostupnih Trinux paketa s kratkim opisom njihove namjene:

4.1. Osnovni paketi

Ovi su paketi potrebni za osnovno funkcioniranje Trinux distribucije te ih je stoga uvijek potrebno učitati. Radi se o sljedećim paketima:

- `system.tgz` – osnovni sistemski alati;
- `baselib.tgz` – skup osnovnih biblioteka potrebnih za funkcioniranje većine aplikacija;
- `dnslibs.tgz` - `libresolv`, `libnsl`, `libnss` biblioteke (potrebne za rad DNS sustava);
- `bash.tgz` – `bash` ljuska;
- `term.tgz` – `ncurses` biblioteke te još neke rutine vezane za rad terminala;
- `pthread.tgz` – još neke GNU biblioteke potrebne za rad većine Trinux aplikacija.

4.2. Opcionalni paketi

Opcionalni paketi koji mogu biti potrebni za rad određenih programa. To su:

- `glib.tgz` – `libglib`, `libgmodule` (biblioteke potrebne za rad `ethereal` programskog paketa);
- `libcpp28.tgz` – `libstdc++.so.2.8.0` moduli potrebni za rad aplikacija pisanih u C++ jeziku.
- `libcpp29.tgz` – `libstdc++-2-libc6.1-1-2.9.0.so` (moduli za C++ aplikacije);
- `libgmp.tgz` – matematičke biblioteke;
- `libdb.tgz` – biblioteke potrebne za rad baza podataka i dijeljenje datoteka (koriste ih `perl`, `dsniff`, itd...).

4.3. Mrežni analizatori

Programi iz ove grupe omogućuju praćenje i analizu mrežnog prometa. U ovu grupu uključeni su sljedeći programi:

- `tcpdump.tgz`
- `ethereal.tgz`
- `ngrep.tgz`
- `ipgrab.tgz`
- `nstreams.tgz`
- `iptraf.tgz`
- `trafshow.tgz`
- `darkstat.tgz`

- ipaudit.tgz
- pof.tgz
- sniffit.tgz
- dsniff.tgz
- utcpdump.tgz
- angst.tgz
- ettercap.tgz
- vomit.tgz

Ovdje nisu dani opisi pojedinih programa, budući da većina njih obavlja slične zadaće vezane za praćenje, analizu te filtriranje mrežnog prometa, provođenje statističkih obrada nad istim i sl.

4.4. Alati za pregledavanje

Alati iz ove skupine namijenjeni su pregledavanju i analizi mrežnih sustava. Uključeni su alati za pregledavanje mrežnih portova (eng. *port scanning*) te alati za ispitivanje pojedinih mrežnih servisa.

- nmap – najpoznatiji alat za pregledavanje mrežnih portova;
- scanners.tgz – nekoliko alata za otkrivanje propusta vezanih za pojedine mrežne protokole (FTP,HTTP; RPC/NFS, DNS ...);
- winscan.tgz – program za analizu NETBIOS protokola;
- xprobe.tgz – detekcija operacijskih sustava putem ICMP protokola;
- arping.tgz – utvrđivanje aktivnosti računala ARP i ICMP paketima;
- icmpenum.tgz – analizator mreže putem ICMP protokola;
- firewalk.tgz – alat za ispitivanje vatrozida;
- telnetftp.tgz – alat za pasivnu identifikaciju sustava na temelju *escape* sekvenci telnet servisa.

4.5. Praćenje neovlaštenih aktivnosti

U ovoj skupini nalaze se programski alati koji omogućuju praćenje i identifikaciju neovlaštenih aktivnosti. Alati ovog tipa poznatiji su pod nazivom **I**ntrusion **D**etection **S**ystems –**IDS**.

- snort – popularni IDS sustav za Linux operacijske sustave;
- sqlsnort.tgz – Snort IDS sustav s podrškom za bilježenje log zapisa unutar MySQL baza podataka;
- pakemon.tgz – još jedan IDS sustav za Linux;
- iplog.tgz – detekcija napada usmjerenih prema Trinux poslužitelju;
- labrea.tgz – program za prevenciju različitih malicioznih aktivnosti;
- despoof.tgz – alat za detekciju lažiranih (eng. *spoofed*) paketa.

4.6. Generatori paketa

Alati koji omogućuju generiranje proizvoljnih TCP/UDP paketa. Budući da i u ovom slučaju svi navedeni alati posjeduju slična svojstva, ovdje je samo navedena njihova lista bez detaljnijeg opisa.

- dnet.tgz
- hping2.tgz
- irpas.tgz
- isic.tgz
- sing.tgz
- fragrour.tgz
- sendip.tgz
- sendpkt.tgz
- mpac.tgz
- nasl.tgz

4.7. Proxy poslužitelji i alati za tuneliranje

- redir.tgz – alat za prosljeđivanje TCP portova (eng. *port forwarding*);

- `tunnel.tgz` – moduli za jezgru i odgovarajući alati koji omogućuju kreiranje IPIP i GRE tunela;
- `httptunl.tgz` – program koji omogućuje prosljeđivanje TCP prometa putem HTTP protokola.

4.8. Programi za enkripciju

- `openssh.tgz` – SSH klijent;
- `opensshd` – SSH poslužitelj;
- `ssldump.tgz` – analizator SSL protokola;
- `stunnel.tgz` – alat za prosljeđivanje i tuneliranje SSL protokola;
- `gnupg.tgz` – *open source* implementacija PGP protokola;
- `openssl.tgz` – alat za generiranje certifikata, zahtjeva za certifikatima, raznih ključeva te ostalih kriptografskih zadaća;
- `zebedee` – program za kriptiranje TCP/UDP prometa.

4.9. Ostali sigurnosni programi

- `zodiac.tgz` – program za lažiranje DNS paketa;
- `sentinel.tgz` – program za detekciju alata za praćenje i analizu mrežnog prometa (eng. *sniffers*);
- `hunt.tgz` – program za provođenje različitih malicioznih aktivnosti (lažiranje paketa, lažiranje mrežnih komunikacijskih veza...).

4.10. Web alati

- `links.tgz` – popularni tekstualni web preglednik koji radi u konzoli;
- `curl.tgz` – višenamjenski klijent za FTP, HTTP, Gopher;
- `wget.tgz` – popularni klijent za dobavljane datoteka (FTP, HTTP);
- `apache.tgz` – najpoznatiji Linux web poslužitelj;
- `authforce.tgz` – alat za *brute-force* napade na Apache web poslužitelje;
- `hammerhead.tgz` – alat za testiranje Apache poslužitelja;
- `webfsd.tgz` – web poslužitelj nešto skromnijih mogućnosti.

4.11. Različiti mrežni alati

- `netconf.tgz` – alati za podešavanje mrežnih parametara (`ipconfig`, `route`...);
- `bind.tgz` – DNS poslužitelj;
- `dhcpcd.tgz` – DHCP klijent;
- `dhcpd.tgz` – DHCP poslužitelj;
- `dhclient.tgz` – još jedan DHCP klijent;
- `echoping.tgz` – alat za mjerenje propusnosti računalne mreže;
- `netutil.tgz` – skup standardnih Linux mrežnih alata (`telnet`, `ftp`, `netstat`, `arp`...);
- `pump.tgz` – DHCP klijent.
- `dnsutil.tgz` – alati za ispitivanje DNS poslužitelja (`dig`, `nslookup`, `whois`...).

4.12. Tekst editori

- `vi` – popularni Linux uređivač teksta;
- `vim` – modificirana inačica spomenutog `vi` editora;
- `nano` – jednostavni uređivač teksta sličan `pico` editoru.

4.13. Alati vezani uz datotečne sustave

Za korištenje većine alata iz ove skupine potrebno je instalirati `ide.tgz` paket. U ovu skupinu uključeni su sljedeći programi:

- `diskutil.tgz` – alati za upravljanje diskom i datotečnim sustavima (`fdformat`, `fdisk`, `lde`...);
- `ext2tools.tgz - e2fsck, mke2fs, badblocks` programi u paketu s potrebnim bibliotekama;
- `fileutil.tgz - bvi, hexdump, strings`;
- `tctbin.tgz` – dio alata iz `Coroner's Toolkit` programa za forenzičku analizu.

4.14. Alati za bežične mreže

- `kismet.tgz` – program za praćenje i analizu prometa na 802.11b kompatibilnim mrežama;
- `wlan-ng.tgz` – programski alati za konfiguraciju `prism` bežičnih kartica.

4.15. Moduli jezgre

Moduli jezgre potrebni za funkcioniranje pojedinih programskih paketa. Moduli su dostupni u obliku paketa te ih je moguće instalirati `getpkg` naredbom čime se olakšava njihovo korištenje.

- `netfilter.tgz` – moduli jezgre potrebni za rad vatrozida;
- `iptables.tgz` – moduli potrebni za programe namijenjene filtriranju mrežnih paketa;
- `usb-core.tgz` – moduli za USB podršku.
- `usb-net.tgz` – dodatni moduli USB podršku.
- `win-fs.tgz` – SMB podrška, *read-only* podrška za NTFS datotečni sustav.
- `linux-fs.tgz` – `ext2`, `ext3`, `reiserfs` podrška.
- `pnp.tgz` – podrška za *Plug and Play* uređaje.

4.16. Ostalo

Alati koji ne spadaju u niti jednu od navedenih skupina.

- `debug.tgz` – programi za otkrivanje grešaka (`strace`, `ltrace`);
- `sysutil.tgz` – razni sistemski programi (`top`, `procinfo`, `si`...).

5. Podizanje Trinux sustava s CDROM-a

Trinux sustav moguće je osim sa disketa podizati i sa CDROM-a. U tu svrhu potrebno je kreirati odgovarajuću `.iso` datoteku te je zapisati na CDROM medij pomoću CD pisača.

Spomenutu `.iso` datoteku moguće je kreirati pomoću `buildiso` skripte ljuske koja je dostupna na web stranicama Trinux projekta (http://trinux.sourceforge.net/release/).

Budući da `buildiso` skripta ljuske za izradu `trinux.iso` datoteke zahtjeva jednu od ranije spomenutih `boot` disketa, potrebno je prethodno u disketni uređaj staviti jednu od njih.

Unutar `/tux/config/pkglist` datoteke na disketi potrebno je navesti sve Trinux pakete koji se žele uključiti u distribuciju. Pokretanjem `buildiso` skripte svi navedeni paketi biti će dobavljeni s Interneta te uključeni u `.iso` datoteku.

S obzirom na kapacitet CDROM medija te nemogućnost naknadnog učitavanja paketa ovim putem, u ovom koraku preporučuje se uključivanje svih onih paketa koji se namjeravaju koristiti. Naime, nakon što je jednom `trinux.iso` datoteka zapisana na CDROM medij, više ne postoji mogućnost dodavanja novih paketa te ih stoga treba pažljivo odabrati.

Dobivenu `.iso` datoteku potrebno je zapisati na CD, nakon čega se isti može koristiti za podizanje Trinux operacijskog sustava (nakon što je u BIOS-u sustava *boot* sekvenca prilagođena za podizanje s CDROM uređaja).

Prije pokretanja `buildiso` skripte preporučuje se njeno prilagođavanje sustavu na kojem se pokreće, a nisu isključene niti sitne izmjene na kôdu kako bi se uspješno obavio postupak kreiranja `.iso` datoteke. Verzija `buildiso` datoteke koja je korištena tijekom testiranja sadržavala je manje pogreške koje su zahtijevale intervenciju na kôdu. Skripta koja je korištena prilikom testiranja dana je u prilogu na kraju dokumenta (Prilog A).

6. Udaljeni pristup

Udaljeni pristup Trinux poslužitelju moguć je putem Secure Shell protokola (`telnet`, `ftp` i slični ostali servisi nisu omogućeni iz sigurnosnih razloga). S obzirom na karakteristike Trinux distribucije ugrađeni SSH poslužitelj ne podržava autentikaciju korisnika putem zaporke, već samo putem parova javni/tajni ključ.

Treba napomenuti da poslužitelj s klijentima komunicira putem 1.99 verzije SSH protokola, što se može smatrati sigurnosnim nedostatkom s obzirom na poznate ranjivosti vezane za tu inačicu protokola.

S obzirom da se autentikacija provodi putem parova javni/tajni ključ, potrebno je na strani klijenta generirati odgovarajući par ključeva (`identity.pub`/`identity`) koji će omogućiti spajanje na poslužitelj. Postupak generiranja spomenutog parova ključeva ovisiti će o korištenom SSH klijentu. Kod Linux operacijskih sustava isti se mogu generirati `ssh-keygen` naredbom.

Nakon što su ključevi generirani i zaštićeni odgovarajućim *passphrase* nizom, potrebno je javni ključ (`identity.pub`) kopirati na disketu u `/etc/tux/pkg/opensshd` direktorij te je preimenovati u ime `keys`. Ukoliko se na Trinux poslužitelj želi spajati s više klijenata potrebno je u datoteci `keys` navesti ključeve svih koji korisnika koji žele pristupati poslužitelju.

Prilikom idućeg podizanja Trinux sustava, na temelju ključeva pohranjenih u `keys` datoteci generirati će se nova `authorized_keys` datoteka koju SSH poslužitelj koristi za autentikaciju korisnika.

Tijekom testiranja mogućnosti udaljenog pristupa otkriven je propust koji otežava pristup SSH poslužitelju. Naime, spomenuta `authorized_keys` datoteka koja se kreira prilikom podizanja sustava inicijalno sadrži neprikladno postavljene ovlasti, koje onemogućuju uspostavu konekcije s SSH poslužiteljem. Problem je u pogrešno postavljenim `w` (`write`) bitovima za grupu i ostale korisnike. Inicijalne ovlasti `authorized_keys` datoteke izgledaju ovako:

```
trinux> ls -al
drwxr-xr-x   2 0        0             192 Nov 18 13:45 .
drwxr-xr-x  19 0        0             704 Dec 10  2000 ..
-rw-rw-rw-   1 0        0             660 Nov 18 13:45 authorized_keys
-rw-------   1 0        0             526 Nov  8 10:43 identity
-rw-r--r--   1 0        0             330 Nov  8 10:43 identity.pub
```

Uz ovako definirane ovlasti poslužitelj je uporno odbijao konekcije klijenata. Nakon što su ovlasti promijenjene na sljedeći način veza je uspostavljena bez problema.

```
trinux> ls -al
drwxr-xr-x   2 0        0             192 Nov 18 13:45 .
drwxr-xr-x  19 0        0             704 Dec 10  2000 ..
-rwxr-xr-x   1 0        0             660 Nov 18 13:45 authorized_keys
-rw-------   1 0        0             526 Nov  8 10:43 identity
-rw-r--r--   1 0        0             330 Nov  8 10:43 identity.pub
```

7. Zaključak

Trinux distribucija pokazala se kao vrlo praktičan alat, budući da sadržava mnoštvo Linux *open source* programa vezanih za administraciju i ispitivanje računalnih mreža i mrežnih servisa.

Ideja RAM diska na kojoj se zasniva cijela Trinux distribucija omogućuje korištenje svih programa u vrlo kratkom vremenu bez potrebe za posebnim prevođenjem i instalacijom svakog programa. Učitavanje paketa može se obaviti na nekoliko načina (Poglavlje 3) od kojih su se kao najzahvalniji pokazali oni putem računalne mreže i CDROM-a. Ukoliko je sve ispravno podešeno Trinux sustav u navedenim situacijama spreman je za korištenje nakon svega nekoliko minuta.

Sustav se pokazao vrlo jednostavnim, pogotovo za korisnike iskusne u radu s Unix/Linux operacijskim sustavima. Učitavanje paketa `getpkg` komandom omogućuje brzo i jednostavno korištenje paketa koji inicijalno nisu uključeni u distribuciju.

S obzirom na provedena testiranja, mišljenje je da Trinux distribucija zahtjeva još dosta poboljšanja i dorada, ali se jednako tako pokazala i kao vrlo perspektivan i dobro zamišljen projekt.

8. Prilog A

`Buildiso` skripta ljuska za izradu `.iso` datoteke.

```
#!/bin/sh

TSRC="/tmp/tux"
PKGSRC="http://trinux.sourceforge.net/pkg/"


#echo "Please modify the shell script for your system"
#exit # delete this


if [ $# = "0" ]
then
        echo "# buildiso prep   - populates source directory"
        echo "# buildiso build  - builds .iso"
        echo "# buildiso burn   - burns to CD"

fi



mkdir $TSRC/trinux 2> /dev/null

if echo $* | grep "prep" > /dev/null
then
        cd $TSRC/trinux
        rm *.tgz 2> /dev/null

        cd $TSRC
        if [ -f boot.img ]
        then
                echo "Found boot image in $TSRC"
        else
                echo "Enter boot floppy"
                read blah
                echo "Creating boot image"
                dd if=/dev/fd0 of=boot.img
        fi

        cd $TSRC/trinux
        echo "Copying files from boot floppy"
        if mount -t vfat /dev/fd0 /floppy
        then
                cp -v -a /floppy/tux .
                cp /floppy/ramdisk .
                cp /floppy/license .
                cp /floppy/version .
                cp /floppy/readme .
                cd /
umount /floppy
        else
                echo "No floppy present"
        fi

                cd $TSRC/trinux
                echo "Retrieving Trinux packages from $PKGSRC"
                cat $TSRC/trinux/tux/config/pkglist

                sleep 2
```

```
                for i in `cat $TSRC/trinux/tux/config/pkglist`
                do
                        wget $PKGSRC${i}.tgz
                done

                [ -f dhcpcd.tgz ] || wget ${PKGSRC}dhcpcd.tgz
                [ -f dnslibs.tgz ] || wget ${PKGSRC}dnslibs.tgz
                [ -f dnslibs.tgz ] || wget ${PKGSRC}system.tgz

                rm *.tgz.1 2> /dev/null
                echo
                echo "Next step:"
                echo "#buildiso build"
fi

if echo $* | grep "build" > /dev/null
then
        pwd
        cd $TSRC
        mkisofs -v -J -o ../trinux.iso -b boot.img .

        echo
        echo "Next step:"
        echo "#buildiso burn"

fi

if echo $* | grep "burn" > /dev/null
then
        cd $TSRC/..
        echo Enter CD-R
        cdrecord -v -dev=0,2,0 -speed=4 trinux.iso
fi
```