HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza grsecurity sigurnosne zakrpe za Linux jezgru

CCERT-PUBDOC-2004-03-67

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

Neizbježni sigurnosni propusti unutar aplikacija, nastali kao pogreška u dizajnu i implementaciji programskog koda ili jednostavno u konfiguraciji same aplikacije, predstavljaju konstantnu prijetnju integritetu operacijskog sustava. Klasične metode rješavanja ovakvih problema svode se na pregledavanje programskog koda u potrazi za spomenutim propustima i njihovo pravovremeno uklanjanje. Ovakav pristup relativno je spor, vrlo skup i nemoguće ga je u potpunosti automatizirati, a krajnji rezultat ne garantira da je softver u potpunosti siguran.

Grsecurity zakrpa za jezgru Linux operacijskih sustava predstavlja skup naprednih metoda zaštite operacijskog sustava, čiji cilj je, za razliku od klasičnih metoda zaštite, prevencija i onemogućavanje iskorištavanja propusta. Osnovna prednost ovakvog pristupa jest njegova univerzalnost, tj. činjenica da štiti od iskorištavanja poznatih ali i još neotkrivenih propusta u aplikacijama.

U sigurnosna poboljšanja koja Grsecurity nudi spadaju:

- Zaštita binarnih datoteka pomoću PaX sustava;
- Zaštita adresnog prostora jezgre;
- Napredne opcije za kontrolu pristupa;
- Zaštita datotečnog sustava;
- Kontrola pokretanja izvršnih datoteka;
- Kontrola pristupa mrežnim resursima;
- Podrška za bilježenje dodatnih log poruka.

Iza navedenih opcija zapravo se kriju mehanizmi zaštite adresnog prostora sustava i aplikacije, napredne kontrole pristupa resursima kao i brojne opcije za obavještavanje i uzbunjivanje administratora putem log poruka. Sve opcije podešavaju se u konfiguracijskom sučelju Linux jezgre, a nakon što se jezgra prevede, određene opcije moguće je kontrolirati i promjenom posebnih parametara prilikom podizanja sustava.

U daljnjem tekstu nastojati će se pobliže objasniti način rada zaštitnih mehanizama i značenje pojedinih konfiguracijskih opcija.

2. Prevođenje Linux jezgre i primjena grsecurity zakrpe

Prije izrade Linux jezgre sa sigurnosnim poboljšanjima, bilo da se radi o grsecurity zakrpi ili o nekom drugom proizvodu, poželjno je imati instaliranu inačicu jezgre koja ispravno radi. Na taj način vrlo je lako eliminirati izvor problema u slučaju da nadograđena jezgra ne radi ispravno. Budući da većina korisnika posjeduje jezgru koja je inicijalno prevedena unutar neke od Linux distribucija, poželjno je prije primjene grsecurity zakrpe, iz izvornog koda, prevesti jezgru Linux operacijskog sustava i testirati njenu ispravnost. U daljnjem tekstu opisati će se standardni postupak prevođenja Linux jezgre i primjena sigurnosnih zakrpi.

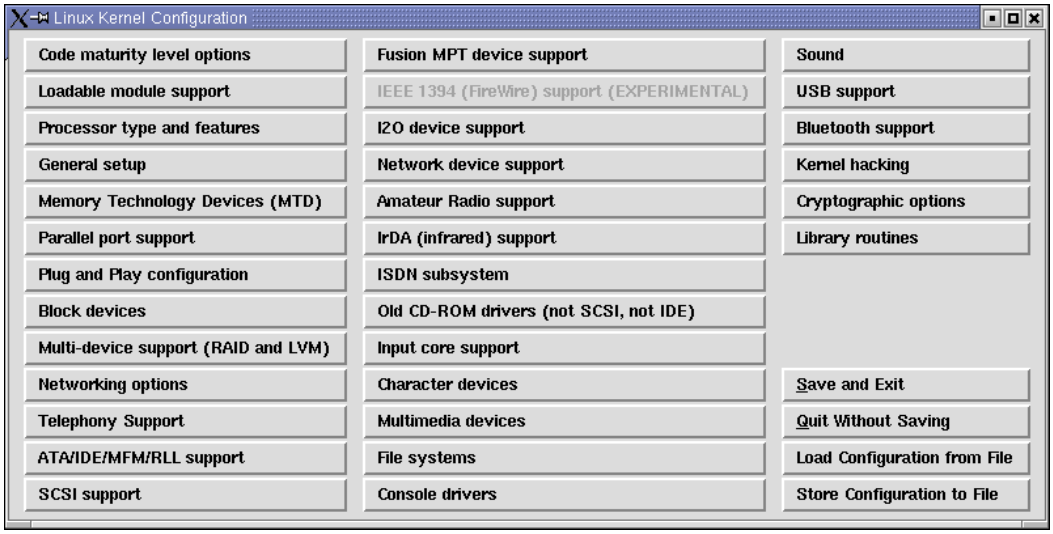
2.1. Prevođenje Linux jezgre

Jezgra je datoteka koja predstavlja najvažniji dio Linux operacijskog sustava, tj. ponaša se kao sučelje između hardvera i softvera i kao podrška za razne mrežne protokole i datotečne sustave. Jezgra je između ostaloga i ono što Linux sustav razlikuje od ostalih UNIX sustava.
Prevođenje programskog koda jezgre u suštini se ne razlikuje od prevođenja programskog koda bilo koje aplikacije. Naravno, budući da se radi o najvažnijem dijelu sustava, bilo kakva greška u postupku uzrokovati će pogrešku pri podizanju sustava. Zbog toga je potrebno u potpunosti razumjeti sve korake prevođenja jezgre i dobro poznavati hardver ugrađen u računalo.
Jezgra se dohvaća sa adrese http://www.kernel.org ili nekog od *mirror* poslužitelja (npr. sunsite.unc.edu). Ukoliko se jezgra dohvaća po prvi puta, potrebno je na lokalno računalo prebaciti cjelokupan izvorni kod paketa označen imenom linux-x.y.zz. Pri čemu x označava glavnu inačicu jezgre (trenutno je u pitanju inačica 2), y označava pod-inačicu glavne inačice (u trenutku pisanja dokumenta 4 i 6), a zz modifikaciju pod-inačice. Neparne vrijednosti parametra y predstavljaju razvojne (nestabilne) inačice jezgre, dok se parne vrijednosti odnose na stabilne pakete. U pravilu, uvijek je potrebno dohvatiti posljednju inačicu stabilne jezgre i kopirati ju u `/usr/src` direktorij.
Ukoliko na računalu već postoji izvorni kod starije inačice jezgre, moguće je sa www.kernel.org stranice dohvatiti samo razliku između dvije inačice jezgre, popularno zvanu zakrpa, te njome nadograditi postojeći kod.
Zakrpa se dodaje pomoću naredbe `patch` na sljedeći način:

```
# patch -p1 < patch-2.4.45
```

Zakrpe za jezgru su inkrementalnog tipa i ukoliko se izvorni kod jezgre na računalu razlikuje nekoliko inačica od posljednje, potrebno je slijedno primijeniti sve objavljene zakrpe.
Kod dohvaćanja izvornog koda jezgre, posebnu pažnju trebaju obratiti korisnici koji izvorni kod jezgre žele instalirati iz distribucijskih rpm ili deb paketa. Naime, zbog razvojne politike navedenih paketa, cjelokupni izvorni kod jezgre podijeljen je u dva zasebna paketa (kernel-source i kernel-headers), od kojih je za uspješno prevođenje jezgre potrebno instalirati oba. Izvorni kod jezgre se po konvenciji smješta unutar `/usr/src` direktorija (iako je moguća i proizvoljna lokacija), nakon čega je u istom direktoriju moguće započeti postupak prevođenja.
Prije bilo kakvih daljnjih koraka potrebno je pokrenuti naredbu `make mrproper`, koja čisti eventualno zaostali programski kod. Otpakirani izvorni kod potrebno je prije prevođenja konfigurirati, što je moguće učiniti korištenjem tri različita pristupa:

1. u tekstualnom komandno linijskom sučelju (`make`);
2. u tekstualnom *ncurses* sučelju (`make menuconfig`);
3. u grafičkom sučelju (`make xconfig`) (**Slika 1**).



Slika 1: *Grafičko sučelje za konfiguraciju jezgre*

Potrebno je napomenuti da je konfiguracija jezgre iz naredbenog retka poprilično kompliciranа i mukotrpna, pa se svakako preporuča korištenje drugog ili trećeg pristupa, što na većini današnjih sustava ne predstavlja problem.

Budući da jezgra sadrži podršku za velik broj protokola i mnoštvo različitog hardvera, korisniku se na odabir nudi više glavnih grupa opcija unutar kojih se nalaze parametri za podešavanje specifične podrške. Podršku za željeni protokol ili hardverski uređaj moguće je uključiti izravno u jezgru ili u obliku modula koji se naknadno učitava po želji. Neke od opcija obavezno se moraju uključiti izravno.

Određen broj opcija inicijalno je već odabran, nudeći na taj način uobičajenu razinu podrške za određen hardver ili protokol. Ukoliko korisnik nije detaljno upoznat sa značenjem ovih opcija, najbolje ih je ostaviti odabrane, jer to predstavlja minimalnu garanciju da će jezgra ispravno funkcionirati. Iskusniji korisnici mogu onemogućiti navedene opcije, kako bi konačna veličina jezgre bila što manja ili kako bi odgovarala njihovim potrebama.

Po završetku postupka konfiguriranja, opcije se pohranjuju u konfiguracijsku (`.config`) datoteku. Naravno, postupak konfiguracije moguće je preskočiti i ručno izmijeniti sadržaj `.config` datoteke, ali ovakav postupak u većini slučajeva završava pogrešno konfiguriranom jezgrom i ne preporučuje se njegovo prakticiranje.

Postupak prevođenja započinje izdavanjem naredbi `make dep` i potom `make clean`. Ove dvije naredbe zadužene su za provjeru ovisnosti prije prevođenja i uklanjanje eventualnih binarnih datoteka zaostalih od prijašnjih prevođenja jezgre.

Jezgra se prevodi naredbom `make bzImage` što će, nakon podužeg postupka prevođenja, rezultirati binarnom datotekom `bzImage` unutar poddirektorija `arch/boot/i386/`. Ova datoteka predstavlja jezgru koja se učitava u radnu memoriju prilikom podizanja sustava. Eventualni moduli prevode se i instaliraju naredbama `make modules` i `make modules_install`.

Prevedenu jezgru potrebno je kopirati na odgovarajuću lokaciju (uobičajeno u `/boot` direktorij) i podesiti *boot loader* program (LILO ili GRUB) da prilikom podizanja sustava učitava novu inačicu jezgre. Pri tome je svakako potrebno pripaziti da se također ostavi mogućnost podizanja posljednje ispravne inačice jezgre, kako bi se u slučaju neispravno prevedene jezgre sustav mogao podići.

Gornji postupak opisuje prevođenje 2.4 inačice jezgre, koja je trenutno najzastupljenija. Identičan postupak, uz manje preinake, primjenjuje se i kod prevođenja inačice 2.6.

Ukoliko se koristi jezgra inačice 2.6, potrebno je obratiti pozornost na inačicu `gcc` prevoditelja i popratnih alata. **Tablica 1** prikazuje preporučene inačice programa i naredbe kojima se one mogu provjeriti.

Alat	Preporučena inačica	Naredba za provjeru inačice
Gnu C	2.95.3	# gcc --version
Gnu make	3.78	# make --version
binutils	2.12	# ld -v
util-linux	2.10	# fdformat --version
module-init-tools	0.9.10	# depmod -V
e2fsprogs	1.29	# tune2fs
jfsutils	1.1.3	# fsck.jfs -V
reiserfsprogs	3.6.3	# reiserfsck -V 2>&1|grep reiserfsprogs
xfsprogs	2.6.0	# xfs_db -V
pcmcia-cs	3.1.21	# cardmgr -V
quota-tools	3.09	# quota -V
PPP	2.4.0	# pppd --version
isdn4k-utils	3.1pre1	# isdnctrl 2>&1|grep version
nfs-utils	1.0.5	# showmount --version
procps	3.1.13	# ps --version
oprofile	0.5.3	# oprofiled –version

***Tablica 1**: Preporučene inačice alata za prevođenje 2.6 jezgre Linux-a*

Postupak konfiguracije praktički je identičan postupku konfiguracije 2.4 jezgre, uz napomenu da se velik dio parametara konfiguracijske datoteke razlikuje, pa se ne preporučuje korištenje stare `.config` datoteke kao polazište kod konfiguracije nove jezgre.

Nakon uspješne konfiguracije izdaje se naredba `make` bez dodatnih parametara, što će rezultirati prevođenjem jezgre i svih dodatni modula. Prevedene module još je potrebno instalirati naredbom `make modules_install`.

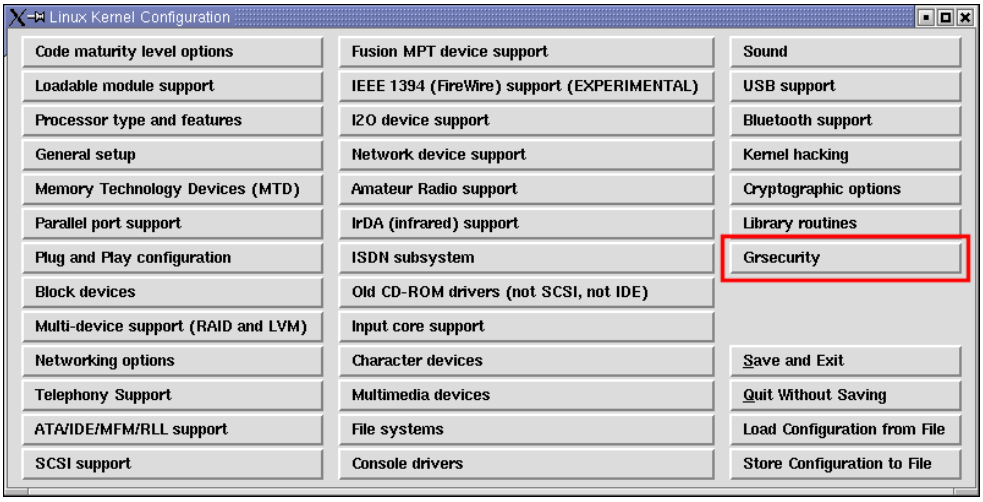
2.2. Primjena grsecurity zakrpe

Izvorni kod zakrpe može se dohvatiti sa adrese http://www.grsecurity.net/download.php, pri čemu je potrebno pripaziti da je inačica jezgre identična onoj za koju je zakrpa namijenjena.

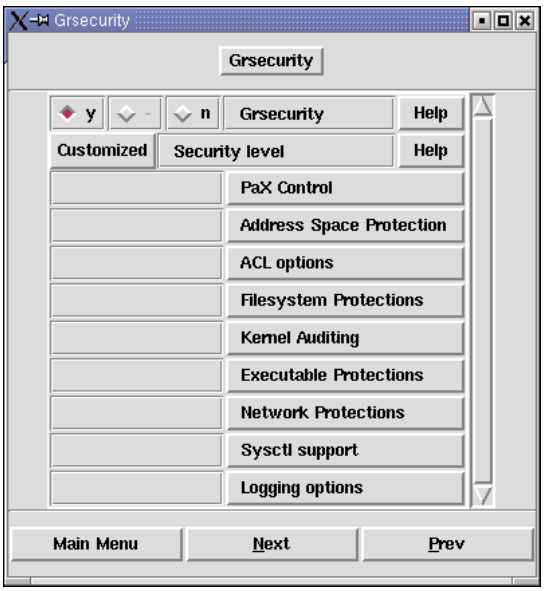
Postupak primjene grsecurity zakrpe nimalo se ne razlikuje od postupka primjene ostalih zakrpi za Linux jezgru (sigurnosne zakrpe, nadogradnje, itd.). Naredbom `patch` dohvaćena grsecurity-1.9.14-2.4.25.patch.txt datoteka uključuje se u kod jezgre.

```
$ patch –p1 < grsecurity-1.9.14-2.4.25.patch
```

Nakon uspješno primijenjene zakrpe, u glavnom izborniku za konfiguraciju jezgre trebalo bi se pojaviti novo polje pod nazivom Grsecurity (**Slika 2**).



Slika 2: *Grafičko sučelje za konfiguraciju jezgre s uključenom grsecurity podrškom*



Slika 3: *Odabir opcija grsecurity zaštite*

Unutar navedenog polja nalaza se sigurnosni dodaci za Linux jezgru (**Slika 3**) čija će se namjena opisati u sljedećim poglavljima. Postupak primjene zakrpe kod 2.6 jezgre identičan je gore opisanom.

3. Podešavanje Grsecurity podrške unutar jezgre

3.1. Automatski odabir opcija

Kako se ne bi pretjerano zamarali sa konfiguracijom gresecurity sigurnosne podrške u Kernelu, manje iskusnim korisnicima ostavljena je mogućnost odabira tri unaprijed podešene razine sigurnosne zaštite. Odabir je napravljen tako da se zadovoljavaju svi potrebni kriteriji sigurnosti za tri slučaja (niski, srednji i visoki), uz uvjet da se zadrži maksimalna kompatibilnost sa klasičnom jezgrom, tj. da nakon primjene grsecurity zakrpe sav softver nesmetano radi.
Uz sve konfiguracijske opcije u daljnjem tekstu navesti će se i izvorni oblik parametra unutar konfiguracijske datoteke jezgre.

3.1.1. Niska razina (CONFIG_GRKERNSEC_LOW)

Niska razina uključuje svega nekoliko opcija za podizanje sigurnosti operacijskog sustava. Opcije su odabrane tako da osiguraju višu sigurnosnu razinu sustava, ali da istovremeno ne ometaju rad aplikacija instaliranih na sustavu. Odabir ove opcije pogodan je za sve korisnike koji na računalu imaju instaliranu veliku količinu različitog softvera koji se ne smatra uobičajenim dijelom Linux distribucija.

3.1.2. Srednja razina (CONFIG_GRKERNSEC_MEDIUM)

Uz sigurnosne restrikcije navedene u niskoj sigurnosnoj razini, srednja sigurnosna razina unosi dodatne sigurnosne mjere. U pravilu, ova razina sigurnosti ne bi trebala stvarati probleme pri radu softvera, ali moguće su nekompatibilnosti sa starijim ili loše napisanim aplikacijama. Ukoliko se koristi ova opcija, administrator sustava mora se pobrinuti da `auth` (`ident`) servis bude pokrenut sa ovlastima grupe *wheel* (GID 10).

3.1.3. Visoka razina (CONFIG_GRKERNSEC_HIGH)

Ova razina, uz opcije navedene u prve dvije razine, uključuje gotovo sve preostale sigurnosne restrikcije koje grsecurity dodatak nudi. Povećana razina sigurnosti predstavlja rizik za kompatibilnost određenih aplikacija. Budući da se kod ove sigurnosne razine uključuju PaX restrikcije, korisniku se preporučuje da prouči dokumentaciju PaX projekta, kako bi bio upoznat sa mogućim posljedicama uključivanja ovih opcija. Kao što je ranije spomenuto, i unutar ove razine potrebno je pokretati `ident` servis sa ovlastima grupe *wheel*.
Tablica 2 prikazuje usporedbu sigurnosnih opcija sve tri razine.

Opcija	Niska razina	Srednja razina	Visoka razina
linking restrictions	✔	✔	✔
fifo restrictions	✔	✔	✔
random pids	✔	✔	✔
Enforcing nproc on execve()	✔	✔	✔
restricted dmesg	✔	✔	✔
random ip ids	✔	✔	✔
enforced chdir("/") on chroot	✔	✔	✔
random tcp source ports	✘	✔	✔
failed fork logging	✘	✔	✔
time change logging	✘	✔	✔
signal logging	✘	✔	✔
deny mounts in chroot	✘	✔	✔
deny double chrooting	✘	✔	✔
deny sysctl writes in chroot	✘	✔	✔
deny mknod in chroot	✘	✔	✔
deny access to abstract AF_UNIX sockets out of chroot	✘	✔	✔

deny pivot_root in chroot	✗	✓	✓
denied writes of /dev/kmem, /dev/mem, and /dev/port	✗	✓	✓
/proc restrictions with special gid set to 10 (usually wheel)	✗	✓	✓
address space layout randomization	✗	✓	✓
removal of addresses from /proc/<pid>/[maps|stat]	✗	✓	✓
additional /proc restrictions	✗	✗	✓
chmod restrictions in chroot	✗	✗	✓
no signals, ptrace, or viewing processes outside of chroot	✗	✗	✓
capability restrictions in chroot	✗	✗	✓
deny fchdir out of chroot	✗	✗	✓
priority restrictions in chroot	✗	✗	✓
segmentation-based implementation of PaX	✗	✗	✓
mprotect restrictions	✗	✗	✓
kernel stack randomization	✗	✗	✓
mount/unmount/remount logging	✗	✗	✓
kernel symbol hiding	✗	✗	✓

Tablica 2: *Pregled sigurnosnih opcija uključenih u tri razine automatskog odabira*

3.2. Ručni odabir opcija

Kako bi ojačana jezgra što bolje odgovarala specifičnim potrebama sustava na koji je instalirana, iskusnijim korisnicima preporučuje se ručno podešavanje svih potrebnih opcija unutar grsecurity zaštite.

3.2.1. Odabir opcija PaX zaštite (PaX Control)

Projekt PaX (http://pax.grsecurity.net/docs/pax.txt) pokrenut je s idejom pronalaženja načina prevencije iskorištavanja sigurnosnih propusta unutar aplikacija, koji napadaču daju ovlasti čitanja i pisanja unutar adresnog prostora napadnute aplikacije. U tu grupu napada najčešće spadaju napadi prepisivanjem spremnika.

Važno je primijetiti da se u ovom slučaju naglasak ne stavlja na pronalaženje i ispravljanje propusta, već se iskorištavanje navedenih propusta pokušava spriječiti. Unutar Grsecurity projekta implementirano je nekoliko zaštitnih mehanizama iz PaX projekta, koje je moguće uključiti sljedećim opcijama:

- **Support soft mode** (CONFIG_GRKERNSEC_PAX_SOFTMODE)
  Omogućavanjem ove opcije pokreće se PaX zaštita u soft načinu rada što podrazumijeva da se sigurnosna zaštita primjenjuje isključivo nad aplikacijama koje su eksplicitno označene pomoću `chpax` naredbe.
  Za korištenje ove opcije obavezno je potrebno uključiti i CONFIG_GRKERNSEC_PT_PAX_FLAGS opciju. Soft način rada moguće je uključiti i prosljeđivanjem kernel opcije `pax_softmode=1` prilikom podizanja sustava, a na sličan način moguće je kontrolirati i ostale PaX opcije u unutar grsecurity jezgre, prosljeđivanjem opcija u `/proc/sys/kernel/pax` datoteku.
- **Use legacy ELF header marking** (CONFIG_GRKERNSEC_PAX_EI_PAX)
  Oblik PaX zaštite može se konfigurirati i na razini samih aplikacija. Ukoliko je binarna datoteka aplikacije u ELF (eng. *Executable Linking File*) formatu, kontrolne zastavice koje određuju ponašanje PaX zaštite smještaju se (pomoću `chpax` naredbe) unutar posebnog dijela zaglavlja ovih datoteka. Ova opcija podržava smještanje zastavica u standardni dio zaglavlja ELF datoteka, što ima određenih nedostataka (npr. nemoguće je uključiti podršku za soft način rada). Bez obzira na to, ova opcija se mora koristiti u slučajevima kada *toolchain* za pokretanje binarnih

datoteka ne podržava drukčiju lokaciju zastavica, ili većina aplikacija ima zastavice smještene na tom mjestu, što čini nezgodnim promjenu njihove lokacije.

- **Use ELF program header marking** (CONFIG_GRKERNSEC_PAX_PT_PAX_FLAGS)
  Iako identična po funkciji kao i prethodna, ova opcija omogućava smještanje zastavica unutar posebnog dijela ELF zaglavlja rezerviranog isključivo za kontrolu PaX zaštite. Ova opcija je naprednija od prethodne i, ukoliko je to moguće, potrebno ju je koristiti. Ukoliko su obje opcije uključene istovremeno, samo ova opcija će se smatrati važećom.
- **MAC system integration** (CONFIG_GRKERNSEC_PAX_NO_ACL_FLAGS)
  MAC (eng. *Mandatory Access Control*) sustavi također imaju mogućnost podešavanja PaX zastavica na razini aplikacije. Ova opcija omogućuje integraciju PaX zaštite u takve sustave, a njene moguće vrijednosti su `none`, `direct` i `hook`, ovisno o vrsti podrške unutar samog sustava.

3.2.2. Zaštita adresnog prostora sustava (eng. *Address Space Protection*)

- **Deny writing to /dev/kmem, /dev/mem, and /dev/port** (CONFIG_GRKERNSEC_KMEM)
  Uključivanjem ove opcije onemogućuje se pisanje po adresnom prostoru jezgre, tj. onemogućuje se izmjena trenutno pokrenute jezgre Linux sustava. Na taj način jezgra se štiti od ubacivanja malicioznog koda. Korištenje ove opcije može rezultirati prekidom rada određenih aplikacija koje za svoj rad neophodno moraju pisati u `/dev/mem`.
- **Disable privileged I/O** (CONFIG_GRKERNSEC_IO)
  Bez obzira na zabranu koju uvodi prethodna opcija, napadač je još uvijek u mogućnosti ubaciti maliciozni kod u jezgru putem `ioperm` i `iopl` poziva. Uključivanjem ove opcije navedeni pozivi vratiti će grešku, što ujedno olakšava i detekciju neovlaštenih aktivnosti na sustavu. Nažalost, i u ovom slučaju, funkcionalnost nekih programa može biti narušena, a tu se prije svega misli na hwclock i XFree86 pakete.
- **Remove addresses from /proc/pid/[maps|stat]** (CONFIG_GRKERNSEC_MEMMAP)
  Uključivanjem ove opcije korisnicima postaju nedostupni podaci navedeni u datotekama `/proc/PID_procesa/maps` i `/proc/PID_procesa/stat`, koji pobliže opisuju korištenje adresnog prostora memorije od strane procesa. Ova naredba izravno je vezana uz korištenje PaX ASLR opcije, budući da uvid u navedene datoteke čini ASLR opciju beskorisnom.
- **Hide kernel symbols** (CONFIG_GRKERNSEC_HIDESYM)
  Ova opcija omogućuje skrivanje informacija o učitanim modulima i kernel simbolima, kojima korisnici inače pristupaju putem `syscall` naredbe.
  Kako bi korištenje ove opcije imalo smisla dodatno je potrebno uključiti napredne ACL opcije koje skrivaju datoteku jezgre sustava i `System.map` datoteku, kao i opcije koje skrivaju sadržaj `/proc/kcore` datoteke. Ukoliko su svi navedeni uvjeti ispunjeni, znatno se smanjuje opasnost od napada na sustav iskorištavanjem propusta u jezgri.

3.2.3. Kontrola pristupa (ACL options)

- **Hide kernel processes** (CONFIG_GRKERNSEC_ACL_HIDEKERN)
  Dodatna zaštita skrivanjem svih procesa pokrenutih od strane jezgre sustava. Uvid u navedene procese biti će dostupan isključivo administratoru.
- **(3) Maximum tries before password lockout** (CONFIG_GRKERNSEC_ACL_MAXTRIES)
  Ovom opcijom definira se maksimalan broj pokušaja prijavljivanja na sustav, tj. pogrešnih prijavljivanja, prije nego se uključi zaštitni mehanizam koji korisniku brani prijavljivanje na određeni vremenski period. Manji broj predstavlja manju mogućnost uspješnog *brute force* napada na sustav.
- **(30) Time to wait after max password tries, in seconds** (CONFIG_GRKERNSEC_ACL_TIMEOUT)
  Ukoliko je prethodna opcija uključena, ovom opcijom definira se vremenski razmak u sekundama koji mora proteći od trenutka kada korisnik prekorači maksimalan broj pogrešnih prijava na sustav do trenutka kada će ponovo biti u mogućnosti prijaviti se.
  Veći vremenski period znatno smanjuje mogućnost *brute force* napada.

3.2.4. Zaštita datotečnog sustava (eng. *Filesystem Protections*)

- **Proc restrictions** (CONFIG_GRKERNSEC_PROC)
  Ova opcija mijenja ovlasti nad datotekama u `/proc` direktoriju, s ciljem podizanja sigurnosti i privatnosti korisnika. Pristup je moguće ograničiti na razini korisnika ili grupe korisnika koja pokreće određeni proces. Korištenje ove opcije može narušiti rad `identd` poslužitelja, ukoliko je pokrenut pod ovlastima drukčijima od administratorskih ili ovlastima grupe definirane ovom opcijom.
- **Linking restrictions** (CONFIG_GRKERNSEC_LINK)
  Uvodi zabranu na korištenje simboličkih linkova unutar direktorija u koji mogu svi korisnici pisati (npr. `/tmp`) onim korisnicima koji nisu vlasnici datoteka na koje pokazuju simbolički linkovi. Na taj način onemogućava se iskorištavanje propusta u aplikacijama koje na nesiguran način stvaraju privremene datoteke.
- **FIFO restrictions** (CONFIG_GRKERNSEC_FIFO)
  Onemogućuje pisanje po FIFO stogovima drugih korisnika, koji se nalaze unutar direktorija u koji mogu svi korisnici pisati.
- **Chroot jail restrictions** (CONFIG_GRKERNSEC_CHROOT)
  Uključivanje ove opcije čini težim probijanje iz *chroot* kaveza aplikacije. Opcija sadrži nekoliko parametara kojima se kontroliraju različite zabrane nad aplikacijama pokrenutima unutar *chroot* kaveza. Neke od restrikcija uključuju zabranu montiranja datotečnih sustava, zabranu izvršavanja `mknod` naredbe, zabranu izvođenja `chmod` naredbe, itd. Ukoliko njihovo korištenje ne narušava rad aplikacija unutar *chroot* kaveza, preporučuje se uključivanje svih ponuđenih opcija.

3.2.5. Napredno praćenja stanja sustava (Kernel Auditing)

Unutar ovog dijela konfiguracije jezgre uključuju se napredne opcije za bilježenje promjena na sustavu u odgovarajuće log datoteke. Pravilnim podešavanjem ponuđenih opcija vrlo je lako detektirati neovlaštene aktivnosti na sustavu ili uočiti nepravilnosti u radu pojedinih aplikacija.

- **Single group for auditing** (CONFIG_GRKERNSEC_AUDIT_GROUP)
  Opcija omogućuje praćenje aktivnosti pojedine grupe korisnika. Konkretno, bilježe se sve `exec`, `chdir`, `(un)mount` i `ipc` aktivnosti specificirane grupe korisnika na sustavu. Korištenje ove opcije olakšava praćenje aktivnosti ciljanih grupa korisnika, što je pogotovo korisno na poslužiteljima koji imaju velik broj korisnika čije je istovremeno praćenje gotovo nemoguće.
- **Exec logging** (CONFIG_GRKERNSEC_EXECLOG)
  Ukoliko je ova opcija uključena sustav će bilježiti sve `execve()` pozive, odnosno pokretanje svake aplikacije na sustavu. Ova opcija vrlo je korisna prilikom praćenja aktivnosti korisnika na sustavu, no potrebno je upozoriti da njeno uključivanje može rezultirati vrlo velikim brojem log poruka, pogotovo na sustavima sa velikim brojem aktivnih korisnika.
- **Resource logging** (CONFIG_GRKERNSEC_RESLOG)
  Bilježi sve pokušaje prekoračenja granica dodijeljenih resursa. U log datoteku upisuje se ime resursa, tražena količina i trenutno postavljeno ograničenje. Uključivanje ove opcije je preporučljivo.
- **Log execs within chroot** (CONFIG_GRKERNSEC_CHROOT_EXECLOG)
  Ova opcija daje mogućnost bilježenja pokretanja svih aplikacija unutar *chroot* kaveza. Slično kao i kod *Exec logging* opcije, moguće je generiranje velikog broja log poruka, što upućuje na oprez prilikom njenog uključivanja.
- **Chdir logging** (CONFIG_GRKERNSEC_AUDIT_CHDIR)
  Bilježi sve `chdir()` pozive na sustavu, tj. promjenu trenutnog direktorija.
- **(Un)Mount logging** (CONFIG_GRKERNSEC_AUDIT_MOUNT)
  Bilježi sva montiranja i demontiranja datotečnih sustava.
- **IPC logging** (CONFIG_GRKERNSEC_AUDIT_IPC)
  Bilježi sve pokušaje stvaranja ili uklanjanja *message queueova*, semafora i dijeljene memorije na sustavu.
- **Signal logging** (CONFIG_GRKERNSEC_SIGNAL)

Omogućuje bilježenje određenih signala na sustavu, poput SIGSEGV, što predstavlja način detekcije neispravnog izvršavanja (rušenja) programa. Korištenjem ove opcije vrlo je lako uočiti neovlaštene aktivnosti na sustavu, poput pokušaja iskorištavanja sigurnosnih propusta unutar određenih aplikacija.

- **Fork failure logging** (CONFIG_GRKERNSEC_FORKFAIL)
  Bilježi sve neuspjele `fork()` pozive, detektirajući na taj način *fork bombing* napade ili pokušaje prekoračenja granica određenog procesa.
- **Time change logging** (CONFIG_GRKERNSEC_TIME)
  Bilježe se svi pokušaji promjene sata sustava.

3.2.6. Kontrola pokretanja izvršnih datoteka (Executable Protections)

- **Enforce RLIMIT_NPROC on execs** (CONFIG_GRKERNSEC_EXECVE)
  Prilikom izdavanja `execve()` poziva provjeravaju se ograničenja resursa korisnika koji je izdao poziv. Na razini sustava ova provjera se trenutno provodi isključivo kod izdavana `fork()` poziva, što u određenim slučajevima omogućuje zaobilaženje restrikcija.
- **Dmesg(8) restriction** (CONFIG_GRKERNSEC_DMESG)
  Korištenje ove opcije onemogućuje upotrebu `dmesg` naredbe za pregledavanje posljednjih 4 kb log poruka unutar spremnika u jezgri svim korisnicima koji nemaju root ovlasti. Na taj način prikrivaju se poruke jezgre generirane prilikom podizanja sustava i inicijalizacije hardvera.
- **Randomized PIDs** (CONFIG_GRKERNSEC_RANDPID)
  Omogućuje generiranje identifikacijskog broja procesa (PID) na temelju pseudo slučajnog algoritma. Na taj način napadač nije u mogućnosti nasumce pogoditi broj procesa određenih poslužitelja, kao ni kojem procesu pripada koja *tmp* datoteka koja se najčešće naziva po PID broju.
- **Trusted path execution** (CONFIG_GRKERNSEC_TPE)
  Predstavlja način kontrole pokretanja aplikacija nad određenim grupama korisnika. Grupe korisnika navedene u ovoj opciji neće biti u mogućnosti pokretati aplikacije koje se nalaze izvan određenih direktorija. Preciznije, pokretati će se samo one aplikacije koje se nalaze u direktorijima čiji vlasnik je administrator i unutar kojih jedino administrator ima pravo pisanja.

3.2.7. Zaštita mrežne komponente sustava (Network Protections)

- **Larger entropy pools** (CONFIG_GRKERNSEC_RANDNET)
  Ovom opcijom poboljšava se postupak generiranja slučajnih brojeva. Budući da se mnoštvo opcija unutar grsecurity zaštite i same jezgre oslanja na korištenje slučajnih brojeva, preporučuje se uključivanje ove opcije.
- **Truly random TCP ISN selection** (CONFIG_GRKERNSEC_RANDISN)
  Postupak generiranja TCP *Initial Sequence* brojeva unutar Linux jezgre nije slučajan, već se TCP ISN broj dobiva postupkom MD4 enkripcije parametara TCP konekcije. Uključivanjem ove opcije, postupak generiranja brojeva biti će identičan onome kod OpenBSD sustava, tj. u potpunosti slučajan.
- **Randomized IP Ids** (CONFIG_GRKERNSEC_RANDID)
  Ukoliko je ova opcija uključena, sva *id* polja odlaznih TCP paketa biti će slučajno odabrana. Slučajan odabir polja ometa rad alata za udaljenu detekciju (eng. *fingerprinting*) operacijskog sustava.
- **Randomized TCP source ports** (CONFIG_GRKERNSEC_RANDSRC)
  Kod određenih TCP konekcija, izvorni port generira se prilikom otvaranja konekcije (eng. *on the fly*), jednostavnim postupkom povećavanja za jedan prethodno otvorenog izvornog porta. Opcija *Randomised TCP source ports* omogućuje slučajno generiranje izvornih portova.
- **Randomized RPC XIDs** (CONFIG_GRKERNSEC_RANDRPC)
  Ova opcija povećava razinu sigurnosti RPC konekcija. Njenim uključivanjem odabir XID brojeva RPC zahtjeva postaje slučajan, što u standardnoj Linux jezgri nije slučaj.

- **Socket restrictions** (CONFIG_GRKERNSEC_SOCKET)
  Korištenjem ove opcije omogućuje se postavljanje zabrane na korištenje mrežnih *socketa* definiranim grupama korisnika. Moguće je zasebno zabraniti korištenje poslužiteljskih i klijentskih *socketa*.

3.2.8. Naknadno podešavanje grsecurity opcija (*Sysctl support*)

Uključivanjem *Sysctl* podrške unutar Grsecurity jezgre korisniku se pruža mogućnost podešavanja sigurnosnih opcija prilikom podizanja sustava. Na ovaj način izbjegava se potreba za ponovnim prevođenjem jezgre u slučaju promjene nekih opcija.
Promjena konfiguracije postiže se pridruživanjem vrijednosti 1 ili 0 parametrima unutar `/proc/sys/kernel/grsecurity` datoteke. Vrijednosti svih opcija inicijalno su postavljene na nulu, tj. isključene su i njihova vrijednost može se mijenjati sve dok se parametru `grsec_lock` ne pridruži vrijednost 1.
Iako uključivanjem ove opcije administrator rješava moguće probleme kod promjene konfiguracije Grsecurity parametara, njezino nepravilno korištenje dovodi maliciozne korisnike u mogućnost manipulacije sigurnosnim postavkama sustava, što umanjuje sve prednosti korištenja Grsecurity zakrpe.
Kako bi se postigla maksimalna razina sigurnosti, unos vrijednosti parametara potrebno je obaviti pri podizanju sustava pomoću posebnih skripti. Skripte moraju biti zaštićene od pisanja i moraju biti napravljene tako da pri završetku podešavanja obavezno vrijednost `grsec_lock` parametra postave na 1.

3.2.9. Kontrola zapisivanja log poruka (eng. *Logging options*)

Kako bi se spriječilo zagušivanje sustava velikim brojem log poruka (kako uobičajenih, tako i specifičnih Grsecurity poruka), ovim skupom konfiguracijskih parametara podešavaju se broj zapisanih poruka u određenom vremenskom intarvalu.

- **(10) Seconds in between log messages (minimum)** (CONFIG_GRKERNSEC_FLOODTIME)
  parametar definira minimalan vremenski razmak između dva zapisivanja grsecurity log poruka. Inicijalno postavljena vrijednost od 10 sekundi vjerojatno će odgovarati u većini slučajeva. Ukoliko postoji potreba za promjenom intervala, potrebno je pripaziti da isti ne bude prevelik, kako bi se poruke uspješno zapisivale, a istodobno parametar mora biti dovoljno velik da se izbjegne preopterećenje sustava
- **(4) Number of messages in a burst (maximum)** (CONFIG_GRKERNSEC_FLOODBURST)
  Za razliku od prethodnog parametra koji definira vremenski interval unutar kojega se zapisuju poruke, ovaj parametar određuje koliki broj log poruka se može zapisati unutar jednog takvog intervala.
  Inicijalna vrijednost također bi trebala odgovarati u većini slučajeva, a potrebno ju je povećati isključivo ako je broj legalnih log poruka toliko velik da se većina interpretira kao preopterećenje.

4. Zaključak

Korištenje sigurnosnih nadogradnji, poput Grsecurity zakrpe, na Linux jezgri efikasan je način zaštite računala od neželjenih lokalnih i udaljenih aktivnosti koje su u stanju ugroziti integritet operacijskog sustava. Grsecurity zakrpa administratorima nudi mnoštvo naprednih opcija, čijim se ispravnim podešavanjem drastično povećava razina sigurnosti Linux operacijskog sustava, a mogućnost automatskog odabira opcija putem više sigurnosnih razina omogućuje primjenu ovog alata i od strane manje iskusnih korisnika. Ispitivanja su pokazala da se korištenje ove zakrpe ne odražava negativno po performanse sustava.

Kao eventualna negativna strana korištenja ovog rješenja može se uzeti u obzir unošenje nesigurnosti u programski kod Linux jezgre. Točnije, ukoliko se otkrije sigurnosni propust unutar programskog koda Grsecurity zakrpe, cijeli sustav automatski postaje ranjiv i moguće je zaobići sve ranije navedene metode zaštite. Ipak, vjerojatnost od pojavljivanja ovakvog propusta vrlo je mala.

Uzevši u obzir sve navedeno, može se zaključiti kako Grsecurity cijenom i jednostavnošću svoje primjene, a u odnosu na razinu sigurnosti koju nudi, uvelike nadmašuje skupe metode ispitivanja programskog koda u potrazi za sigurnosnim propustima i naknadnu primjenu sigurnosnih zakrpa.