Sigurnost Linuxa KAKO

Kevin Fenzi, *kevin@scrye.com* i Dave Wreski, *dave@nic.com* verzija 0.9.11, 1. svibnja 1998.

Ovaj je dokument općenit pregled sigurnosnih problema s kojima je suočen administrator Linux sustava. Pokriva općenitu filozofiju sigurnosti i više specifičnih primjera boljeg osiguravanja vašeg Linux sustava od uljeza. Spominju se i drugi izvori informacija i programa o sigurnosti. NAPOMENA: ovo je beta verzija ovog dokumenta. Poboljšanja, konstruktivne kritike, dodatke i ispravke zahvalno prihvaćamo. Pošaljite svoje poruke i jednom i drugom autoru. Nemojte zaboraviti "Linux", "security" ili "HOWTO" u Subject: liniji svoje poruke kako bi izbjegli spam filtere i brzo dobili pažnju autora.

Sadržaj

1 Uvod

Ovaj dokument pokriva neke od glavnih problema sigurnosti koji utječu na sigurnost Linuxa. Govori se o općoj filozofiji i resursima na mreži.

S problemima sigurnosti preklapa se više drugih KAKO dokumenata i, gdje je prikladno, na njih ste upućeni.

Ovaj dokument NIJE svjež popis sigurnosnih rupa. Puno novih stalno se pojavljuje. Ovaj će vam dokument reći gdje da potražite svježe informacije i izložiti neke općenite metode sprečavanja takvih rupa.

1.1 Nove verzije ovog dokumenta

Nove verzije ovog dokumenta redovito se šalju u *comp.os.linux.answers*. Također se dodaju raznim anonimnim FTP serverima koji takve informacije arhiviraju, uključujući `<ftp://sunsite.unc.edu/pub/Linux/docs/HOWTO/>`.

Ovaj bi dokument trebali moći naći i na Linux WWW stranici na `<http://sunstie.unc.edu/mdw/linux.html>`.

Na kraju, najsvježije verzije ovog dokumenta trebale bi biti dostupne u raznim formatima s `<http://scrye.com/~kevin/lsh/>`.

1.2 Komentari

Sve komentare, greške, dodatne informacije i kritike svih vrsta šaljite na *kevin@scrye.com* i *dave@nic.com*.

NAPOMENA: molimo vas, poruku pošaljite obojici. Provjerite da li je u Subject:-u poruke "Linux", "security" ili "HOWTO" da izbjegnete Kevinov spam filter.

1.3 Odricanje

Za sadržaj ovih dokumenata ne prihvaćamo nikakvu odgovornost. Ideje, primjere i drugi sadržaj koristite na svoju odgovornost. Također, ovo je nedovršena verzija, s mnogim mogućim netočnostima i greškama.

Dosta primjera i opisa koriste Red Hat(TM)-ov sustav pakiranja i izgled sustava. Vaš ne mora biti jednak.

Opisani su samo programi koji se pod određenim uvjetima mogu koristiti ili iskušati za osobne svrhe. Većina programa dostupna je u potpunosti, s izvornim kodom, pod GNU-olikim uvjetima.

1.4 Informacije o autorskim pravima

Ovaj dokument je (C) 1998. Kevin Fenzi i Dave Wreski, a distribuira se pod slijedećim uvjetima:

- KAKO dokumente može se reproducirati i distribuirati u cjelosti ili djelomično, na mediju fizičkom ili elektroničkom, dok je ova obavijest na svim primjercima. Komercijalna distribucija dopuštena je i ohrabrena; međutim, autor bi o takvom distribuiranju želio biti obaviješten.
- Svi prijevodi, izvedeni ili sažeti radovi koji uključuju Linux KAKO dokumente moraju biti pod ovom licencom. Dakle, ne smijete napraviti rad izveden iz KAKO-a i nametati dodatna ograničenja na njegovu distribuciju. Iznimke ovim pravilima moguće su pod određenim uvjetima; kontaktirajte Linux KAKO koordinatora na dolje danoj adresi.
- Ako imate pitanja, kontaktirajte Tima Bynuma, Linux KAKO koordinatora, na *linux-howto@sunsite.unc.edu*.

2 Pregled

Ovaj dokument pokušava objasniti neke postupke i često korištene programe koji vaš Linux čine sigurnijim. Važno je da prvo razjasnimo neke osnovne stvari, da steknete temeljna znanja iz sigurnosti prije nego počnemo.

2.1 Što će nam sigurnost?

U promijenjivom svijetu globalnih podatkovnih komunikacija, jeftinih veza na Internet i vrlo brzog razvoja softvera, sigurnost postaje sve važnija. Sigurnost je sada osnovna potreba jer je globalno računalstvo po prirodi nesigurno. Na primjer, dok vaši podaci idu iz točke A u točku B na Internetu, možda će usput proći kroz nekoliko drugih točaka, dajući drugim korisnicima priliku da presreću, i čak mijenjaju, vaše podatke. Čak i drugi korisnici na vašem sustavu mogu zloćudno pretvarati vaše podatke u nešto neželjeno. Neodobreni pristup vašem sustavu mogu dobiti uljezi, takozvani **crackeri**, koji zatim koriste svoje napredne vještine u imitiranju vas, u krađi podataka od vas, ili čak onemogućavanju pristupa vašim vlastitim resursima. Ako se još uvijek pitate koja je razlika između **hackera** i crackera, pročitajte **How to Become A Hacker** (kako postati haker) Erica S. Raymonda na `<http://sagan.earthspace.net/~esr/faqs/hacker-howto.html>`.

2.2 Koliko je sigurno sigurno?

Najprije, imajte na umu da nijedan računalni sustav nikad ne može biti "potpuno siguran". Sve što možete je otežati kompromitiranje vašeg sustava. Za prosječnog kućnog korisnika Linuxa, ne treba puno da obični kreker ostane na lancu. Za velike Linux korisnike (banke, telekomunikacijske tvrtke, itd.) potrebno je mnogo više posla.

Drugi faktor kojeg treba uzeti u obzir je da, što je vaš sustav sigurniji, sigurnost vam sve više smeta. U tom balansiranju trebate naći točku gdje je vaš sustav moguće koristiti, ali je još siguran za vaše potrebe. Na primjer, mogli biste od svih koji se na vaš sustav spajaju telefonskom vezom tražiti da vaš sustav nazove njih na njihov kućni broj. To jest sigurnije, ali ako netko nije kod kuće, teško će se logirati. Također biste mogli svoj Linux sustav ostaviti bez mreže ili veze na Internet, ali to vrlo otežava surfanje WWW-om.

Ako ste sustav veće ili srednje veličine, trebali bi razviti "Sigurnosnu politiku" o tome koliko sigurnosti vaš sustav zahtijeva i kojim se postupkom ona provjerava. Dobro poznati primjer sigurnosne politike možete naći na `<http://ds.internic.net/rfc/rfc2196.txt>`. Nedavno je osvježen i sadrži izvrsnu podlogu za sigurnosnu politiku vaše tvrtke.

2.3 Što pokušavate zaštititi?

Prije nego pokušate osigurati svoj sustav, trebate odlučiti kolika je prijetnja protiv koje se morate zaštititi, koje rizike biste ili ne biste trebali podnijeti i koliko će na kraju vaš sustav biti ranjiv. Proučite svoj sustav i saznajte što i zašto štitite, koliko je to vrijedno i tko je odgovoran za vaše podatke i drugo vlasništvo.

- Rizik je mogućnost da uljez uspije u pokušaju pristupa vašem računalu. Može li uljez čitati, pisati datoteke, ili izvršavati programe koji bi vam mogli naštetiti? Može li važne podatke obrisati? Spriječiti vas ili vašu tvrku da obavite važne poslove? Ne zaboravite, netko s pristupom vašem računu ili sustavu također se može predstavljati kao vi.

  Zatim, jedan nesiguran račun na vašem sustavu može dovesti do kompromitiranja cijele vaše mreže. Jedan korisnik kojem je dopušteno logiranje preko `rhosts` datoteke, ili nesigurna usluga, kao što je tftp, rizik je koji uljezu omogućava da "prođe kroz vrata". Kada uljez jednom dobije korisnički račun na vašem sustavu ili sustavu nekog drugog, može ga koristiti za dobivanje pristupa drugom sustavu, ili drugom računu.

- Obično vam prijeti netko tko želi neodobren pristup vašoj mreži ili računalu. Odlučite kome vjerujete dovoljno da ima pristup vašem računalu, i koju bi on prijetnju mogao predstavljati.

  Evo nekoliko vrsta uljeza. Korisno je misliti na različite osobine dok osiguravate svoje sustave.

  Znatiželjni

  Ovu vrstu uljeza zapravo zanima koju vrstu sustava i podataka imate.

Zloćudni

Ova vrsta uljeza želi ili srušiti vaše sustave, ili unakaziti vašu WWW stranicu, ili vam drukčije oduzeti vrijeme i novac za oporavak.

Uljez koji se hoće istaći

Ova vrsta uljeza pokušava preko vašeg sustava doći do popularnosti ili slave. Može vaš važan sustav koristiti za razglašavanje svoje sposobnosti.

Konkurencija

Ove uljeze zanima koje podatke imate na sustavu. Možda misle da imate nešto što bi im dobro došlo financijski ili drugačije.

- Ranjivost opisuje koliko je dobro vaše računalo zaštićeno od drugih mreža i mogućnost neodobrenog pristupa.

  Što je na kocki ako netko provali u vaš sustav? Naravno da brige kućnog korisnika dinamičkog PPP-a nisu jednake brigama tvrtke koja svoje računalo spaja na Internet ili drugu veću mrežu.

  Koliko bi vam vremena trebalo da ponovo nabavite/napravite izgubljene podatke? Vrijeme uloženo sada može spasiti deset puta više vremena poslije ako budete morali ponovno stvoriti podatke koje izgubite. Jeste li u zadnje vrijeme provjerili svoju strategiju backupa i svoje podatke?

2.4 Razvijanje sigurnosne politike

Napravite jednostavnu, općenitu politiku za svoj sustav, koju vaši korisnici mogu lako razumjeti i poštovati. Ona treba zaštititi podatke koje čuvate, kao i privatnost korisnika. Neke stvari koje biste mogli dodati je tko ima pristup sustavu (može li moj prijatelj koristiti moj račun?), kome je dozvoljeno da na sustav instalira softver, tko posjeduje koje podatke, oporavljanje od katastrofe i prikladno korištenje sustava.

Opće prihvaćena sigurnosna politika počinje frazom:

> Što nije dozvoljeno zabranjeno je.

To znači da ako korisniku ne date pristup usluzi, on je ne smije koristiti dok pristup ne dobije. Provjerite da li to funkcionira na vašem običnom korisničkom računu – reći "ma ne mogu shvatiti ovaj problem s dozvolama, idem jednostavno biti root" može dovesti do vrlo očitih sigurnosnih rupa, čak i dosad nepoznatih.

2.5 Načini osiguravanja vašeg sustava

Ovaj dokument će govoriti o raznim sredstvima osiguravanja stvari za koje ste toliko radili: vaše lokalno računalo, podatke, korisnike, mrežu, čak i vaš ugled. Što će se dogoditi s vašim ugledom ako uljez obriše podatke nekog vašeg korisnika? Ili vam unakazi WWW stranice? Ili objavi poslovne planove vaše tvrke za slijedeći kvartal? Ako planirate mrežnu instalaciju, mnogo faktora treba uzeti u obzir prije dodavanja ijednog računala.

Čak i ako imate jednostavan PPP račun ili malen sustav, to ne znači da uljeze ne zanimate. Veliki, istaknuti sustavi nisu jedine mete – mnogi uljezi jednostavno žele iskoristiti što više sustava bez obzira na njihovu veličinu. Također mogu koristiti sigurnosnu rupu u vašem sustavu za pristup drugim sustavima kojima ste spojeni.

Uljezi imaju mnogo vremena i mogu izbjeći pogađanje načina na koji ste osigurali sustav jednostavnim isprobavanjem svih mogućnosti. Ima još nekoliko razloga zbog kojih bi se uljez mogao zanimati za vaše sustave o kojima ćemo govoriti poslije.

2.5.1 Sigurnost računala

Možda se najviše brige za sigurnost troši na pojedina računala. To obično znači provjeravanje sigurnosti vašeg sustava uz nadu da svi ostali na mreži rade isto. Odabir dobrih lozinki, osiguravanje usluga lokalne mreže vašeg poslužitelja, pažljivo održavanje korisničkih računa i nadogradnja programa s poznatim sigurnosnim rupama dio su odgovornosti lokalnog sigurnosnog administratora. Iako je to potpuno nužno, postaje težak zadatak ako vaša mreža računala postane veća.

2.5.2 Sigurnost vaše mreže

Sigurnost mreže potrebna je koliko i sigurnost lokalnog računala. Uz vaš sustav, ili distribuiranu računalnu mrežu, Internet, ili stotine, ako ne i tisuće računala na istoj mreži ne možete računati na sigurnost svakog od njih. Provjeravanje dozvola samo provjerenim korisnicima za korištenje vaših mrežnih resursa, građenje firewalla, korištenje jake enkripcije i provjere da nema izloženih ili nesigurnih računala na vašoj mreži sve su dio dužnosti mrežnog sigurnosnog administratora.

Ovaj će dokument govoriti o nekim tehnikama za osiguravanje vašeg sustava u nadi da vam pokaže neke načine sprečavanja pristupanja uljeza u ono što pokušavate zaštititi.

2.5.3 Sigurnost pomoću opskurnosti

Jedna vrsta sigurnosti koju je potrebno raspraviti je "sigurnost preko opskurnosti". To se odnosi na stvari poput mijenjanja imena 'root' u 'toor' kako bi se otežala provala u vaš sustav kao root – osjećaj sigurnosti je lažan i dovest će do vrlo neugodnih posljedica. Budite sigurni da će svaki napadač na sustav brzo progledati kroz takve prazne sigurnosne mjere. To što imate malen sustav ili niste istaknuti ne znači da se uljezi neće zanimati za ono što imate. U slijedećim dijelovima govorit ćemo o onome što štitite.

2.6 Organizacija ovog dokumenta

Ovaj dokument podijeljen je na više dijelova. Oni pokrivaju razne vrste sigurnosnih problema. Prvi, o fizičkoj sigurnosti, govori o zaštiti vašeg računala od fizičkog petljanja. Drugi opisuje kako zaštititi vaš sustav od petljanja lokalnih korisnika. Treći, o datotekama i sigurnosti datotečnog sustava, pokazuje kako namjestiti datotečne sustave i dozvole na vašim datotekama. Slijedeći, o sigurnosti preko lozinki i enkripcije, govori o korištenju enkripcije za bolju sigurnost vašeg računala i mreže. Sigurnost kernela govori o mogućnostima kernela koje biste trebali koristiti ili biti svjesni za sigurniji stroj. Sigurnost mreže opisuje kako bolje osigurati svoj Linux sustav od napada s mreže. Sigurnosne pripreme govori o pripremanju vašeg/ih računala prije nego što ih umrežite. Slijedeći dio govori što poduzeti kada otkrijete provalu sustava u toku ili koja se nedavno dogodila. Zatim su nabrojeni drugi izvori informacija o sigurnosti, a na kraju su neka pitanja i odgovori i nekoliko završnih riječi.

Dvije važne stvari koje trebate shvatiti čitajući ovaj dokument su:

- Budite svjesni svog sustava. Provjeravajte logove sustava kao što je `/var/log/messages` i pazite na svoj sustav, i
- Drugo, držite svoj sustav svježim instaliranjem trenutnih verzija softvera i nadogradnjama zbog sigurnosnih opasnosti. To će vaš sustav učiniti znatno sigurnijim.

3 Fizička sigurnost

Prvi "sloj" sigurnosti kojeg trebate uzeti u obzir je fizička sigurnost vaših računalnih sustava. Tko ima izravan fizički pristup vašem računalu? Da li bi trebao? Možete li zaštititi svoje računalo od njegova petljanja? Da li biste trebali?

Koliko fizičke sigurnosti trebate za svoj sustav jako ovisi o vašoj situaciji i/ili financijama.

Ako ste kućni korisnik, vjerovatno vam je ne treba puno (iako ćete možda htjeti zaštititi svoje računalo od djece ili neugodnih rođaka). Ako ste u laboratoriju, treba vam poprilično više, no korisnici na računalima ipak moraju moći raditi. Mnogi od slijedećih dijelova bit će od pomoći. Ako ste u uredu, trebat će vam ili neće osiguravanje računala dok ne radite ili dok ste na putu. U nekim tvrtkama ostavljanjem neosigurane konzole možete zaraditi otkaz.

Očite metode fizičke sigurnosti kao što su brave na vratima, kablovima, zaključani kabineti i video kamere sve su dobra ideja, ali izvan dosega ovog dokumenta. :)

3.1 Računalne brave

Mnoga moderna PC kućišta imaju mogućnost "zaključavanja". To je obično brava na prednjem dijelu kućišta u kojoj dobiveni ključ možete okrenuti u zaključani ili nezaključani položaj. Brave na kućištima mogu pomoći u sprečavanju krađe vašeg PC-a, ili otvaranja kućišta i izravnog mijenjanja/krađe vašeg hardvera. Nekad mogu spriječiti i resetiranje vašeg računala uz dizanje sustava s diskete ili drugog hardvera.

Te brave rade različite stvari, ovisno o podršci matične ploče i konstrukciji kućišta. Na mnogim PC-ima napravljene su tako da kućište morate slomiti kako bi ga otvorili. Na drugima ne možete uključivati nove tipkovnice i miševe. Za više informacija provjerite upute svoje matične ploče ili kućišta. To ponekad može biti vrlo korisna mogućnost, iako su brave obično niske kvalitete i vrlo ih je lako otključati otpiračem.

Neka kućišta (najizraženije Sparcovi i Macovi) imaju kuku otraga tako da, ako provučete kabel, napadač mora prerezati kabel ili slomiti kućište da bi ga otvorio. Stavljanje šifre ili brave može biti dobra odbrana od krađe stroja.

3.2 BIOS sigurnost

BIOS je najniža razina softvera koja konfigurira ili radi s vašim x86 baziranim hardverom. LILO i druge metode dizanja Linuxa pristupaju BIOS-u kako bi odlučile kako dignuti vaše Linux računalo. Druge platforme na kojem Linux radi imaju sličan softver (OpenFirmware na Macovima i novijim Sunovima, Sun boot prom, itd.). Preko BIOS-a možete spriječiti napadača u resetiranju vašeg računala i mijenjanju vašeg Linux sustava.

Pod Linuxom/x86 mnogi PC BIOS-i daju vam mogućnost lozinke pri dizanju sustava. To ne znači baš puno sigurnosti (BIOS se može resetirati, ili maknuti ako netko može do unutrašnjosti kućišta), ali može poslužiti kao dobra obrana (to jest, potrajat će i ostaviti tragove petljanja).

Mnogi x86 BIOS-i omogućavaju i određivanje raznih drugih dobrih sigurnosnih mjera. Provjerite priručnik svog BIOS-a ili ga razgledajte prilikom slijedećeg dizanja. Neki primjeri: isključivanje dizanja s disketa i lozinke za pristup nekim opcijama BIOS-a.

Na Linux/Sparc-u vaš SPARC EEPROM može se namjestiti da zahtijeva lozinku pri dizanju. To će možda usporiti napadača.

NAPOMENA: Ako imate poslužitelj i stavite lozinku pri dizanju, vaš se stroj neće dizati samostalno. Nemojte zaboraviti da ćete morati doći i dati lozinku čak i kod nestanka struje. ;(

3.3 Sigurnost programa za dizanje

Razni programi za dizanje Linuxa također mogu imati lozinku. Ako koristite LILO, pogledajte opcije **restricted** i **password**. **password** vam traži lozinku pri dizanju. **restricted** će dopustiti dizanje sustava *osim* ako netko odredi opcije na `LILO:` promptu (kao što je **single**).

Naravno, pri postavljanju svih tih lozinki trebat ćete ih i popamtiti. :) Također nemojte zaboraviti da će one samo usporiti odlučnog napadača. To neće spriječiti da netko digne sustav s diskete i montira vašu root particiju. Ako koristite sigurnost uz svoj program za dizanje sustava, možete odmah i u BIOS-u svog računala isključiti dizanje s diskete, kao i zaštiti ga lozinkom.

Ako netko ima informacije o sigurnosti drugih programa za dizanje, rado bismo ih čuli (grub, silo, milo, linload, itd.).

NAPOMENA: Ako imate poslužitelj i stavite lozinku pri dizanju, vaš se stroj neće dizati samostalno. Nemojte zaboraviti da ćete morati doći i dati lozinku čak i kod nestanka struje. ;(

3.4 xlock i vlock

Ako s vremena na vrijeme odlutate od svog stroja, lijepo je moći "zaključati" svoju konzolu da nitko ne petlja po njoj ili gleda što ste radili. Ovo mogu dva programa: xlock i vlock.

xlock zaključava X prikaz. Trebao bi doći sa svakom Linux distribucijom koja podržava X. Za više opcija provjerite njegovu man stranicu, ali općenito možete pokrenuti xlock iz bilo kojeg xterma na svojoj konzoli i on će zaključati prikaz i tražiti lozinku za otključavanje.

vlock je jednostavan mali program kojim zaključavate neke ili sve virtualne konzole na svojem Linux stroju. Možete zaključati samo onu u kojoj radite ili sve. Ako zaključate samo jednu, drugi mogu doći i koristiti konzolu, ali ne i vaš vty dok ga ne otključate. vlock dolazi s Red Hat Linuxom, ali to ne mora vrijediti za vašu distribuciju.

Naravno da će zaključavanje konzole spriječiti petljanje drugih u vaš posao, ali ne spriječava resetiranje stroja ili prekid vašeg posla na neki drugi način. Također ne spriječava pristup vašem računalu s drugog računala na mreži i uzrokovanje problema.

3.5 Otkrivanje fizičkih provala

Prva stvar na koju uvijek treba paziti je kad se vaš stroj digneo. Pošto je Linux robustan i stabilan OS, stroj bi se trebao ponovo dizati kada ga VI spustite za nadogradnje OS-a, izmjenu hardvera ili nešto slično. Ako se stroj digneo bez vašeg sudjelovanja, trebalo bi se upaliti svjetlo za uzbunu. Mnogi načini kompromitiranja vašeg računala zahtijevaju da ga uljez resetira.

Provjerite znakove petljanja na kućištu i području računala. Iako mnogi uljezi iz logova čiste tragove svoga prisustva, dobra je ideja provjeriti ih i potražiti bilo kakve nejasnosti.

Neke stvari koje trebate provjeriti u logovima:

- Kratki ili nepotpuni logovi.
- Logovi s čudnim oznakama vremena.
- Logovi s netočnim dozvolama ili vlasništvom.
- Znakovi ponovnog dizanja sustava ili uključivanja usluga.
- Nedostajući logovi.

- su zapisi ili logini iz čudnih mjesta.

O podacima iz logova sustava govorit ćemo kasnije.

4 Lokalna sigurnost

Slijedeća stvar koju trebate pogledati je osigurnost vašeg sustava protiv napada lokalnih korisnika. Jesmo li mi to rekli *lokalnih* korisnika? Da.

Dobivanje pristupa lokalnom korisniku jedna je od prvih stvari koju uljezi u sustav pokušaju na svom putu do rootovog računa. Uz nedostatke lokalne sigurnosti, zatim mogu "nadograditi" svoj obični korisnički pristup do administratora kroz razne bagove i jadno namještene lokalne usluge. Ako svoju lokalnu sigurnost učinite dobrom, uljez će naići na još jednu prepreku.

Lokalni korisnici mogu uzrokovati dosta štete na vašem sustavu čak i (posebno) ako su stvarno oni za koje se predstavljaju. Davanje računa ljudima koje ne poznajete ili za koje nemate kontaktnih informacija vrlo je loša ideja.

4.1 Stvaranje novih računa

Korisničke račune trebali biste davati zadovoljavajući samo minimalne potrebe zadatka koji obavljaju. Ako svom desetgodišnjem sinu date račun, možda ćete htjeti da on ima pristup samo word procesoru ili programu za crtanje i ne može brisati tuđe podatke.

Nekoliko dobrih pravila procjenjivanja kod dopuštanja pristupa drugih ljudi vašem Linux stroju:

- Dajte im minimalne privilegije koje su im potrebne.
- Budite svjesni kada/od kamo se logiraju, ili bi se trebali logirati.
- Budite sigurni i zbrišite njihov račun kada im više nije potreban.

Mnogi računi lokalnih korisnika koji se koriste u provalama sigurnosti nisu korišteni mjesecima ili godinama. Pošto ih nitko ne koristi, idealno su sredstvo napada.

4.2 Sigurnost roota

Najtraženiji račun na vašem računalu je račun administratora. On ima vlast nad cijelim strojem, a možda i nad drugim strojevima na mreži. Sjetite se da bi rootov račun trebali koristiti samo za vrlo kratke, određene zadatke, a uglavnom biti obični korisnik. Biti root cijelo vrijeme vrlo vrlo vrlo je loša ideja.

Nekoliko trikova da ne zabrljate svoj vlastiti stroj dok ste root:

- Kada pokrećete neku složenu naredbu, prvo je pokušajte pokrenuti u ne-destruktivnom načinu... Posebno naredbe koje koriste nadopunjavanje: tj., ako hoćete pokrenuti `rm foo*.bak`, umjesto toga prvo napišite `ls foo*.bak` i provjerite da li ćete obrisati neželjene datoteke. Korištenje naredbe `echo` umjesto destruktivnih naredbi također ponekad pomaže.
- Neki ljudi misle da tu pomaže `touch /-i`. Tako će vas naredbe poput `rm -rf *` pitati da li stvarno želite obrisati sve te datoteke. (Zato što vaša ljuska prvo nadopuni datoteku `-i` koju rm tretira kao opciju.) To neće pomoći kod rm naredbi bez `*`. ;(
- Postanite root samo za pojedine posebne zadatke. Ako ne znate kako nešto napraviti, vratite se u ljusku običnog korisnika dok niste *sigurni* što root treba obaviti.

- Staza je vrlo važna za root korisnika. Naredbena staza, odnosno PATH varijabla okružja, određuje mjesta na kojima ljuska traži prorgame. Pokušajte ograničiti stazu za root korisnika što je više moguće i nikad nemojte koristiti `.`, odnosno "trenutni direktorij", u svojem PATH-u. Također nemojte u PATH-u imati direktorije u koje se može pisati jer to omogućava napadačima mijenjanje ili smještanje novih izvršnih datoteka u vašu naredbenu stazu tako da postanu root slijedeći put kada vi pokrenete tu naredbu.
- Nikad nemojte koristiti rlogin/rsh/rexec (takozvane **`r-utilities`**) alate kao root. Oni su podložni mnogim napadima i vrlo opasni kada ih pokreće root. Nikad ne stvarajte `.rhosts` datoteku za roota.
- Datoteka `/etc/securetty` sadrži popis terminala s kojih se root može logirati. Tu su predefinirane (na Red Hat Linuxu) samo virtualne konzole (vty-i). Budite vrlo pažljivi kod dodavanja bilo čega drugog ovoj datoteci. Trebali biste moći logirati se s daljine kao obični korisnik, a zatim, ako trebate, `su` (po mogućnosti preko ssh-a ili drugog enkriptiranog kanala), tako da nema potrebe za mogućnošću izravnog logiranja kao root.
- Uvijek budite spori i odlučni dok ste root. Vaši postupci mogu utjecati na mnogo stvari. Razmislite prije tipkanja!
- Ako svakako morate dopustiti nekome (po mogućnosti vrlo provjerenom) nadkorisnički pristup na vašem računalu, ima nekoliko alata koji vam mogu pomoći. sudo omogućava korisnicima da koriste svoju lozinku za pristup ograničenom skupu naredbi kao root. Na primjer, to omogućava korisniku da izbacuje i montira pokretljive medije na vašem Linux stroju, ali nema drugih root privilegija. sudo ima i logove svih uspješnih i neuspješnih pokušaja pokretanja tako da možete otkriti tko je za što koristio koju naredbu. Zato sudo dobro radi čak i na mjestima gdje više ljudi ima pristup rootu tako da se mogu vidjeti počinjene promjene.

  Iako se sudo može koristiti za davanje određenih privilegija određenom korisniku za određene zadatke, ima nekoliko nedostataka. Trebalo bi ga koristiti samo za ograničen skup zadataka, kao što ponovno pokretanje servera ili dodavanje novih korisnika. Svaki program koji nudi izlaz u ljusku dat će korisniku pristup rootu. Na primjer, to vrijedi za većinu editora. Također, nevin program poput `/bin/cat` može se koristiti za prepisivanje datoteka tako da se pristup rootu može zloćudno iskorištavati. sudo smatrajte sredstvom za vođenje računa i ne očekujte da zamijeni roota i uz to bude siguran.

5 Sigurnost datoteka i datotečnog sustava

Nekoliko minuta pripreme i planiranja prije uključivanja u mrežu može pomoći u zaštiti sustava i podataka koji su na njima pohranjeni.

- Ne bi trebalo biti razloga za dopuštanje pokretanja SUID/SGID programa iz korisničkih home direktorija. Za particije na koje mogu pisati drugi osim roota koristite `nosuid` opciju u `/etc/fstab`. Možda ćete iskoristiti i `nodev` i `noexec` na korisničkim home particijama, kao i na `/var`, koje zabranjuju izvršavanje programa i stvaranje znakovnih ili blok uređaja, koji ionako ne bi trebali biti potrebni.
- Ako izvozite datotečne sustave preko NFS-a, konfigurirajte `/etc/exports` sa što je više moguće restriktivnim pristupom. To znači nekorištenje metaznakova, nedopuštanje pisanja na / i montiranje samo-za-čitanje kad god je moguće.
- Konfigurirajte korisnički umask za stvaranje datoteka što restriktivnije. Uobičajene su vrijednosti 022, 033, te najograničenija 077, a dodaju se u `/etc/profile`.
- Umjesto predefiniranog `unlimited` stavite granice na zauzeće datotečnog sustava. Ograničenja po korisniku možete mijenjati korištenjem resource-limits PAM modula i `/etc/pam.d/limits.conf`. Na primjer, ograničenja za grupu `korisnici` mogla bi izgledati ovako:

```
@korisnici     hard  core    0
@korisnici     hard  nproc   50
@korisnici     hard  rss     5000
```

Ovo zabranjuje stvaranje `core` datoteka, ograničava broj procesa na 50 i korištenje memorije na 5 MB po korisniku.

- Datoteke `/var/log/wtmp` i `/var/run/utmp` sadrže zapise o logiranju svih korisnika sustava. Cjelovitost ove datoteke mora se održati jer se ona preko nje možete saznati kada i od kamo je korisnik (ili mogući uljez) ušao na vaš sustav. Ove datoteke također bi trebale imati dozvole 644, bez utjecaja na normalan rad sustava.

- `immutable` bit može se koristiti za sprečavanje slučajnog brisanja ili prepisivanja datoteke koja mora biti zaštićena. Također sprečava simboličko vezanje na tu datoteku, što su koristili napadi brisanja `/etc/passwd` i `/etc/shadow`. Za više informacija o `immutable` bitu pogledajte man stranicu chattr(1).

- SUID i SGID datoteke na vašem sustavu mogući su sigurnosni rizik i pažljivo ih treba pratiti. Zbog toga što ti programi daju posebne privilegije korisniku koji ih je pokrenuo, potrebno je osigurati da se nesigurni programi ne instaliraju. Omiljeni krekerski trik je iskoristiti SUID root programe, a zatim ostaviti SUID program kao stražnji ulaz za slijedeći put, čak i ako je izvorna rupa začepljena.

  Nađite sve SUID/SGID programe na svom sustavu i pratite njihovo stanje, tako da ste svjesni bilo kakvih promjena koje bi mogle značiti mogućeg uljeza. Koristite slijedeću naredbu za traženje svih SUID/SGID programa na sustavu:

```
root# find / -type f \( -perm -04000 -o -perm -02000 \)
```

  Slobodno pomoću chmod(1) maknite SUID ili SGID dozvole na sumnjivom programu, a zatim ih vratite ako baš bude potrebno.

- Datoteke u koje svi mogu pisati, pogotovo datoteke sustava, mogu biti sigurnosna rupa ako kreker pristupi vašem sustavu i izmijeni ih. Također, direktoriji u koje svi mogu pisati opasni su jer omogućuju krekeru da po želji dodaje ili briše datoteke. Za lociranje svih datoteka u koje svi mogu pisati koristite ovu naredbu:

```
root# find / -perm -2 -print
```

  i provjerite zašto svi mogu pisati u njih. Tokom normalnog rada bit će nekoliko takvih datoteka, uključujući neke iz `/dev` i simboličke veze.

- Datoteke bez vlasnika također mogu pokazati da je uljez pristupio vašem sustavu. Datoteke koje nemaju vlasnika ili ne pripadaju grupi možete naći naredbom:

```
root# find / -nouser -o -nogroup -print
```

- Traženje `.rhosts` datoteka također bi trebalo biti dio vaših uobičajenih dužnosti administratora jer one ne bi smjele biti dopuštene na vašem sustavu. Zapamtite, kreker treba samo jedan nesiguran račun da možda dobije pristup vašoj cijeloj mreži. Sve `.rhosts` datoteke na sustavu možete naći ovom naredbom:

```
root# find /home -name .rhosts -print
```

- Na kraju, prije mijenjanja dozvola na bilo kojoj datoteci sustava, budite sigurni da znate što radite. Nikad ne mijenjajte dozvole datoteci jer to izgleda kao lak način za rješavanje problema. Uvijek odlučite zašto datoteka ima takve dozvole prije nego što ih promijenite.

5.1 Postavljanje umaska

Naredba umask može se koristiti za mijenjanje predefiniranih dozvola stvorenih datoteka. To je oktalni komplement željenog moda datoteke. Ako se datoteke stvaraju bez ikakve brige o njihovim dozvolama, korisnik bi mogao nenamjerno dati dozvole za čitanje ili pisanje nekome tko ih ne bi trebao imati. Tipični umaskovi su 022, 027 i 077 koji je najrestriktivniji. Obično se umask postavlja u `/etc/profile` tako da vrijedi za sve korisnike sustava. Na primjer, možda imate red koji izgleda ovako:

```
# Postavlja predefinirani umask korisnika
umask 033
```

Provjerite da li je umask roota 077, što će isključiti dozvole za čitanje, pisanje ili izvršavanje drugim korisnicima, osim ako ih izričito ne promijenite preko chmod(1).

Ako koristite Red Hat i njihov način stvaranja ID-ova korisnika i grupa (**User Private Groups** – osobne grupe korisnika), za umask je dovoljno koristiti 002, zahvaljujući činjenici da je svaki korisnik u svojoj grupi.

5.2 Dozvole datoteka

Važno je osigurati da vaše datoteke sustava nisu otvorene editiranju korisnika i grupa koji takvu administraciju ne trebaju obavljati.

UNIX razdvaja kontrolu pristupa datotekama i direktorijima po tri osobine: vlasnik, grupa i ostali. Vlasnik može biti samo jedan, grupa može imati bilo koliko članova, te svi ostali.

Brzo objašnjenje UNIX dozvola:

Vlasništvo:

Koji korisnik/ci i grupa/e ima/ju kontrolu nad postavljanjem dozvola za datoteku i njenog roditelja.

Dozvole:

Bitovi sposobni za namještanje ili resetiranje koji omogućuju određene vrste pristupa. Dozvole za direktorije mogu imati drukčije značenje od jednakih dozvola datoteka.

Čitanje:

- sposobnost pregledavanja sadržaja datoteke
- sposobnost pregledavanja direktorija

Pisanje:

- sposobnost dodavanja podataka ili mijenjanja datoteke
- sposobnost brisanja i micanja datoteka u direktoriju

Izvršavanje:

- sposobnost pokretanja izvršne datoteke ili skripte ljuske
- sposobnost traženja u direktoriju, uz dozvolu za čitanje

`Save Text` **atribut: (za direktorije)**

Ljepljivi (**sticky**) bit kod direktorija također ima drukčije značenje. Ako je postavljen na direktoriju, korisnik smije brisati samo datoteke koje posjeduje ili za koje ima izričitu dozvolu za pisanje, čak i kada ima dozvolu za pisanje u direktorij. Ovo je napravljeno za direktorije poput `/tmp` u koje svi mogu pisati, ali gdje nije poželjno da bilo koji korisnik po volji briše datoteke. Ljepljivi bit prikazuje se kao `t` u dugom ispisu direktorija.

SUID atribut: (za datoteke)

Ovo opisuje **set-user-id** (postavi ID korisnika) dozvole datoteke. Kada je SUID mod pristupa uključen u dozvolama vlasnika i datoteka izvršna, procesi koji ju pokrenu dobivaju pristup resursima sustava koje ima vlasnik datoteke. To je uzrok mnogih buffer overflow rupa.

SGID atribut: (za datoteke)

Ako je postavljen u dozvolama grupe, taj bit kontrolira **set-group-id** stanje datoteke. Ponaša se kao i SUID, osim što se odnosi na grupu. Da bi to imalo učinka datoteka također mora biti izvršna.

SGID atribut: (za direktorije)

Ako SGID bit uključite na direktoriju (preko `chmod g+s direktorij`), datoteke stvorene u tom direktoriju imat će grupu koju ima direktorij.

Vi

vlasnik datoteke

Grupa

grupa kojoj pripadate

Svi

svi na sustavu, osim vlasnika i članova grupe

Primjer na datoteci:

```
-rw-r--r--  1 kevin  korisnici     114 Aug 28  1997 .zlogin
1. bit - direktorij?               (ne)
 2. bit - čitanje za vlasnika?      (da, za kevina)
  3. bit - pisanje za vlasnika?      (da, za kevina)
   4. bit - izvršavanje za vlasnika?  (ne)
    5. bit - čitanje za grupu?         (da, za korisnici)
     6. bit - pisanje za grupu?         (ne)
      7. bit - izvršavanje za grupu?     (ne)
       8. bit - čitanje za sve?           (da, za sve)
        9. bit - pisanje za sve?           (ne)
         10. bit - izvršavanje za sve?      (ne)
```

Evo primjera minimalnih položaja dozvola koji su potrebni za opisane radnje. Možda ćete htjeti dati više dozvola, ali ovo pokazuje što znače te minimalne dozvole:

`-r----`	Vlasniku dopušta čitanje datoteke
`-w----`	Vlasniku dopušta mijenjanje i brisanje datoteke
`--x---`	Vlasnik može izvršiti ovaj program, ali ne skriptu ljuske, kojoj još treba dozvola za čitanje
`--s---`	Izvršit će se uz UID vlasnika
`----s-`	Izvršit će se uz GID vlasnika
`-rw---T`	Ne osvježava se "vrijeme zadnje promjene". Obično se koristi za swap datoteke
`--t---`	Bez učinka (bivši ljepljivi bit).

Primjer na direktoriju:

```
drwxr-xr-x  1 kevin  korisnici     114 Aug 28  1997 .zlogin
1. bit - direktorij?              (da, s puno datoteka)
 2. bit - čitanje za vlasnika?      (da, za kevina)
  3. bit - pisanje za vlasnika?      (da, za kevina)
   4. bit - izvršavanje za vlasnika?  (da, za kevina)
    5. bit - čitanje za grupu?         (da, za korisnici)
     6. bit - pisanje za grupu?         (ne)
      7. bit - izvršavanje za grupu?     (da, za korisnici)
       8. bit - čitanje za sve?           (da, za sve)
        9. bit - pisanje za sve?           (ne)
         10. bit - izvršavanje za sve?      (ne, za sve)
```

Evo primjera minimalnih položaja dozvola koji su potrebni za opisane radnje. Možda ćete htjeti dati više dozvola, ali ovo pokazuje što znače te minimalne dozvole:

`dr----`	Sadržaj se može pregledati, ali ne se atributi ne mogu pročitati
`d-x---`	U direktorij se može ući i koristiti u potpunim stazama za izvršavanje
`dr-x---`	A sada atribute može čitati vlasnik
`d-wx---`	Sad se datoteke mogu stvarati/brisati, čak i ako direktorij nije trenutni
`d---x-t`	Sprečava brisanje datoteka od strane drugih korisnika s mogućnošću pisanja. Koristi se za `/tmp`
`d--s-s-`	Bez učinka

Konfiguracijske datoteke sustava (obično u `/etc` obično imaju dozvole 640 (`-rw-r---`) i posjeduje ih root. Ovisno o sigurnosnim potrebama vašeg sustava to možete i promijeniti. Nikad ne ostavljajte dozvolu za pisanje grupe ili sviju na datoteci sustava. Neke konfiguracijske datoteke, kao što je `/etc/shadow`, trebao bi moći čitati samo root, a direktoriji u `/etc` trebali bi biti barem nedostupni ostalima.

SUID skripte ljuske

SUID skripte ljuske ozbiljan su sigurnosni rizik i zato ih kernel neće kao takve izvršavati. Ma koliko vi mislili da je ona sigurna, takvu skriptu mogu iskoristiti krekeri za dobivanje root pristupa.

5.3 Provjera cjelovitosti pomoću Tripwirea

Još jedan dobar način otkrivanja lokalnih (a i mrežnih) napada na vaš stroj je provjera cjelovitosti, kao što je Tripwire. Tripwire izračunava niz checksumova za sve vaše važne programe i konfiguracijske datoteke i uspoređuje ih s podacima o prijašnjim, dobro poznatim vrijednostima. Tako će se pokazati sve promjene datoteka.

Dobra je ideja instalirati Tripwire na disketu i zatim je fizički zaštititi od pisanja. Na taj način uljezi ne mogu petljati sa samim Tripwireom ili mijenjati podatke. Kad Tripwire jednom namjestite, dobro je pokretati ga kao dio vaših normalnih dužnosti sigurnosnog administratora da vidite da li nešto promijenjeno.

Čak možete dodati crontab zapis koji svake noći pokreće Tripwire s diskete i šalje vam rezultate. Nešto kao:

```
# postavljamo adresu
MAILTO=kevin
# pokrećemo Tripwire
15 05 * * * root /usr/local/adm/tcheck/tripwire
```

poslat će vam izvještaj svakog jutra u 5:15.

Tripwire je dar s neba za otkrivanje uljeza prije nego što biste ih inače primjetili. Pošto se na prosječnom sustavu mijenja mnogo datoteka, morate pažljivo razlikovati aktivnost krekera i svoj vlastiti rad.

5.4 Trojanski konji

Trojanski konj dobio je ime po poznatoj prijevari iz Homerovog velikog književnog djela. Ideja je u tome da napravite program ili izvršnu datoteku koja izgleda sjajno i koju će drugi ljudi nabaviti i pokrenuti kao root. Zatim možete kompromitirati njihov sustav dok ne paze. Dok oni misle da program koji su upravo skinuli radi jedno (a to može biti i istina), on također poništava osiguranje.

Pazite koje programe instalirate na svoje računalo. Red Hat nudi MD5 provjeru i PGP potpise, RPM datoteke tako da se možete uvjeriti da instalirate pravu stvar. Druge distribucije imaju slične metode. Nikad ne pokrećite program za kojeg nemate izvornog koda ili dobro poznatu izvršnu datoteku kao root! Malo će napadača izvorni kod izložiti oku javnosti.

Iako to može biti dosta složeno, provjerite da li izvorni kod programa nabavljate s izvornog mjesta distribucije. Ako ćete ga pokretati kao root, provjerite sami ili netko kome vjerujete izvorni kod.

6 Sigurnost lozinki i enkripcija

Jedna od najvažnijih načina osiguranja koji se koriste u današnje vrijeme su lozinke. Važno je da vi i svi vaši korisnici imate sigurne, nepogodive lozinke. Većina novijih Linux distribucija dolaze s programom passwd koji ne dopušta lozinke koje je lako pogoditi. Provjerite da li je vaš passwd svjež i da li ima takve mogućnosti.

Dublje ulaženje u temu enkripcije izvan je dosega ovog dokumenta, ali potreban je barem uvod. Enkripcija je vrlo korisna, možda čak i potrebna u ovakvom dobu. Postoji mnogo načina enkriptiranja podataka, svaki sa svojim osobinama.

Većina Unixa (ni Linux nije iznimka) za enkriptiranje lozinki primarno koriste jednosmjerni algoritam enkriptiranja zvan DES (**D**ata **E**ncryption **S**tandard – standard enkripcije podataka). Takve enkriptirane lozinke pohranjuju se u (obično) `/etc/passwd` ili (neuobičajenije) `/etc/shadow`. Kada se pokušate logirati, što god upišete ponovo se enkriptira i uspoređuje s zapisom u datoteci u kojoj su vaše lozinke. Ako se slažu, to mora biti ista lozinka i ulaz vam je dopušten. Iako je DES dvosmjeran algoritam enkripcije (možete enkriptirati i dekriptirati poruku ako imate prave ključeve) varijanta koju većina Unixa koristi jednosmjerna je. Dakle, ne bi trebalo biti moguće obrnuti smjer enkripcije i dobiti lozinku iz sadržaja `/etc/passwd` (odnosno `/etc/shadow`).

Napadi grubom silom kao što je Crack ili John the Ripper (v. dolje) često pogode lozinke ako one nisu dovoljno slučajne. PAM moduli (v. dolje) omogućavaju korištenje različitog načina enkripcije lozinki (MD5 ili slično).

O izabiranju dobre lozinke možete pročitati na `<http://consult.cern.ch/writeup/security/security_3.html>`.

6.1 PGP i kriptografija javnih ključeva

Kriptografija javnih ključeva, koju koristi i PGP, koristi jedan ključ za enkripciju i jedan za dekripciju. Tradicionalno, kriptografija koristi za enkripciju isti ključ kao i za dekripciju. Taj "osobni ključ" mora biti poznat obje strane i na neki način sigurno prenesen od jedne do druge.

Kriptografija javnih ključeva poništava potrebu sigurnog prenošenja ključa koji se koristi za enkripciju pomoću korištenja dva odvojena ključa, javnog ključa i osobnog ključa. Javni ključ svake osobe dostupan je svakome za enkripciju, no osobni ključ ima samo ta osoba kako bi dekriptirala poruke šifrirane točnim javnim ključem.

I kriptografija javnih i kriptografija osobnih ključeva imaju svoje prednosti – o tim razlikama govori se u **RSA Cryptography FAQ**, navedenom na kraju ovog dijela.

PGP (**P**retty **G**ood **P**rivacy – prilično dobra privatnost) na Linuxu je dobro podržan. Verzije 2.6.2 i 5.0 dobro funkcioniraju. Za dobar uvod u PGP i kako ga koristiti pogledajte **PGP FAQ**, `<http://www.pgp.com/service/export/faq/55faq.cgi>`. Pazite da uzmete verziju koja odgovara vašoj zemlji, jer se prema ograničenjima izvoza iz SAD-a jaka enkripcija smatra vojnim oružjem i njeno prenošenje u elektronskom obliku izvan zemlje je zabranjeno.

Tu je i vodič korak-po-korak u konfiguriranju PGP na Linuxu, koji se može naći na `<http://mercury.chem.pitt.edu/~angel/LinuxFocus/English/November1997/article7.html>`. Napisan je za međunarodnu verziju PGP-a, ali lako se primjeni na verziju za SAD. Možda će vam trebati i zakrpa za neke od najnovijih Linux verzija koja se može naći na `<ftp://sunsite.unc.edu/pub/Linux/apps/crypto>`.

Više informacija o kriptografiji može se naći u **RSA Cryptography FAQ** na `<http://www.rsa.com/rsalabs/newfaq/>`. Tu ćete naći informacije o stvarima kao što je "Diffie-Hellman", "kriptografija javnih ključeva", "digitalne potvrde", itd.

6.2 SSL, S-HTTP, HTTPS i S/MIME

Korisnike često zanimaju razlike između raznih sigurnosnih i enkripcijskih protokola, te njihovo korištenje. Iako ovo nije dokument o enkripciji, bilo bi dobro da razjasnimo što je što i gdje naći više informacija.

SSL:

(**S**ecure **S**ockets **L**ayer) metoda je enkripcije koju je razvio Netscape za sigurnost preko Interneta. Podržava nekoliko različitih enkripcijskih protokola i omogućava autentifikaciju klijenta i poslužitelja. SSL radi na razini prijenosa stvarajući sigurni kanal podataka i tako može transparentno enkriptirati mnoge vrste podataka. To ćete najčešće vidjeti pregledavajući u Communicatoru siguran dokument sa sigurnog poslužitelja, a služi kao osnova sigurnih komunikacija pomoću Communicatora, kao i mnoge druge enkripcije podataka Netscape Communicationsa. Više informacija može se naći na `<http://www.consensus.com/security/ssl-talk-faq.html>`. Informacije o drugim Netscapeovim sigurnosnim implementacijama i dobra početna točka za ove protokole nalazi se na `<http://home.netscape.com/info/security-doc.html>`.

S-HTTP:

S-HTTP je još jedan protokol koji omogućava sigurne usluge preko Interneta. Napravljen je da pruži povjerljivost, provjerenost, cjelovitost i nezamjenjivost istovremeno podržavajući mehanizme za rad s više ključeva i kriptografske algoritme kroz pregovaranje opcija između strana umiješanih u svaku transakciju. S-HTTP je ograničen na poseban program koji ga implementira i svaku poruku posebno enkriptira. (iz **RSA Cryptography FAQ**, str. 138)

S/MIME

- S/MIME, odnosno **S**ecure **M**ultipurpose **I**nternet **M**ail **E**xtension, enkripcijski je standard koji se koristi za enkriptiranje elektronske pošte i drugih tipova poruka preko Interneta. To je otvoren standard kojeg razvija RSA, pa se nadamo da ćemo ga uskoro vidjeti i na Linuxu. Više informacija o S/MIME-u može se naći na `<http://home.netscape.com/assist/security/smime/overview.html>`.

6.3 Linux x-kernel – implementacija IPSEC-a

Uz CIPE i druge oblike enkripcije podataka, za Linux postoji i implementacija IPSEC-a. IPSEC je rezultat napora IETF-a u stvaranju kriptografski sigurnih komunikacija na razini IP mreža, koji također pruža autentifikaciju, cjelovitost, kontrolu pristupa i povjerljivost. Informacije o IPSEC-u i Internet nacrtu mogu se naći na `<http://www.ietf.org/html.charters/ipsec-charter.html>`. Tamo su i veze na druge protokole koji rade s ključevima, te IPSEC mailing lista i arhive.

Linux implementacija koja se razvija na Sveučilištu Arizone koristi x-kernel, objektno bazirani okvir za implementiranje mrežnih protokola, a može se naći na `<http://www.cs.arizona.edu/xkernel/hpcc-blue/linux.html>`. Najjednostavnije rečeno, x-kernel je način prenošenja poruka na razini kernela, što olakšava implementaciju.

Kao i drugi oblici kriptografije, ne distribuira se zajedno s kernelom zbog ograničenja u izvozu.

6.4 SSH, stelnet

SSH (**S**ecure **Sh**ell – sigurna ljuska) i stelnet su programi koji vam omogućavaju rad na udaljenim sustavima kroz enkriptiranu vezu.

SSH je skup programa koji se koriste kao sigurna zamjena za rlogin, rsh i rcp. Za enkriptiranje između dva računala koristi kriptografiju javnih ključeva, kao i za provjeru korisnika. Može se koristiti za sigurno logiranje na udaljeno računalo ili kopiranje podataka između računala ujedno sprečavajući napade između (**session hijacking** – otimanje sesije) i DNS **spoofing** (varanje). Sažimat će vaše veze i osiguravati X11 veze između računala. SSH-ove WWW stranice su `<http://www.cs.hut.fi/ssh/>`.

SSH možete koristiti i sa svoje Windows radne stanice na svoj Linux SSH poslužitelj. Ima nekoliko besplatnih Windows implementacija klijenta, uključujući onu na `<http://guardian.htu.tuwien.ac.at/therapy/ssh/>`, kao i komercijalnu implementaciju DataFellowsa na `<http://www.datafellows.com>`.

SSLeay je besplatna implementacija Netscapeovog Secure Sockets Layer protokola, kao i nekoliko aplikacija, kao što je Secure telnet, modul za Apache, nekoliko baza podataka, te nekoliko algoritama uključujući DES, IDEA i Blowfish.

Koristeći taj library napravljena je sigurna zamjena za telnet koja enkriptira telnet vezu. Za razliku od SSH-a, stelnet koristi SSL, **S**ecure **S**ockets **L**ayer, koji je razvio Netscape. Secure telnet i Secure FTP možete naći počevši od **SSLeay FAQ**, dostupnog na `<http://www.psy.uq.oz.au/~ftp/Crypto/>`.

6.5 PAM - Pluggable Authentication Modules

Novije verzije distribucije Red Hat Linux isporučuju se s jedinstvenom shemom autentifikacije zvanom "PAM". PAM vam omogućava mijenjanje metoda i potreba autentificiranja u letu te enkapsuliranje svih lokalnih autentifikacijskih metoda bez ponovnog kompajliranja ijednog programa. Konfiguracija PAM-a je izvan dosega ovog dokumenta, ali potrudite se i pogledajte WWW stranice PAM-a za više informacija. `<http://www.kernel.org/pub/linux/libs/pam/index.html>`

Samo neke od stvari koje možete s PAM-om:

- Koristiti nešto što nije DES za enkripciju svojih lozinki (što ih čini težim za probijanje grubom silom).
- Postaviti ograničenja korištenja za sve svoje korisnike tako da ne mogu izvoditi **denial of service** napade (broj procesa, količina memorije, itd.).
- Uključiti shadow lozinke u letu.
- Određenim korisnicima dozvoliti da se logiraju samo u određeno vrijeme s određenog mjesta.

Samo nekoliko sati nakon instaliranja i konfiguriranja svog sustava možete spriječiti mnoge napade prije nego što se i dogode. Na primjer, koristite PAM za isključivanje korištenja `.rhosts` datoteka na sustavu u home direktorijima korisnika dodavanjem ovih redova `/etc/pam.d/login`:

```
#
# Korisnicima onemogućavamo rsh/rlogin/rexec
#
login auth required pam_rhosts_auth.so no_rhosts
```

6.6 Kriptografska IP enkapsulacija (CIPE)

Najvažniji cilj ovog softvera je pružiti mogućnost sigurne (od prisluškivanja, kao i analiza prometa, te ubacivanja krivotvorenih poruka) veze podmreža preko nesigurne paketne mreže kao što je Internet.

CIPE (**C**ryptographic **IP E**ncapsulation) podatke enkriptira na mrežnoj razini. Paketi koji putuju između računala enkriptirani su. Enkripcija se izvodi blizu same podrške koja šalje i prima pakete.

To je različito od SSH-a koji podatke enkriptira na vezi, na razini socketa. Logička veza između programa na različitim računalima enkriptirana je.

CIPE se može koristiti za **tunnelling** kako bi stvorili **Virtual Private Network** (virtualnu privatnu mrežu). Enkripcija na niskom nivou ima prednost što može transparentno raditi između dvije mreže spojene u VPN, bez ikakvog mijenjanja aplikacija.

Sažeto iz dokumentacije CIPE-a:

IPSEC standardi definiraju skup protokola koje se može koristiti (među ostalim) za izgradnju enkriptiranih VPM-ova. Međutim, IPSEC je relativno težak i složen skup protokola s mnogo opcija, potpune implementacije još uvijek se rijetko koriste, a neka pitanja (kao što je rad s ključevima) još nisu do kraja riješena. CIPE koristi jednostavniji pristup u kojem se mnoge stvari (kao što je izbor algoritma enkripcije) mogu promijeniti samo pri instalaciji. To ograničava prilagodljivost, ali omogućava jednostavnu (i zato djelotvornu, u kojoj je lako pronaći greške) implementaciju.

Više informacija može se naći na `<http://www.inka.de/~bigred/devel/cipe.html>`.

Kao i drugi oblici kriptografije, ne distribuira se s kernelom zbog ograničenja u izvozu.

6.7 Kerberos

Kerberos je sustav autentifikacije koji je razvio Athena projekt na MIT-u. Kada se korisnik logira, Kerberos ga autentificira (preko lozinke) i daje mu način dokazivanja identiteta drugim poslužiteljima i računalima razbacanim na mreži.

Ovu autentifikacija često koriste programi kao što je rlogin kako bi korisniku omogućili logiranje na druga računala bez lozinke (umjesto datoteke `.rhosts`). Autentifikaciju također koristi sustav pošte kako bi se zajamčila isporuka pošte pravoj osobi, kao i istinit identitet pošiljatelja.

Ukupni učinak instaliranja Kerberosa i brojnim drugih programa koji s njime dolaze je gotovo potpuna eliminacija mogućnosti da korisnik prevari sustav da je netko drugi. Nažalost, instalacija Kerberosa vrlo je temeljita i zahtijeva promjene ili zamjene mnogih standardnih programa.

Više informacija o Kerberosu može se naći na `<http://www.veritas.com/common/f/97042301.htm>`, a izvorni kod na `<http://nii.isi.edu/info/kerberos/>`.

(iz **Stein, Jennifer G., Clifford Neuman, and Jeffrey L. Schiller. "Kerberos: An Authentication Service for Open Network Systems." USENIX Conference Proceedings, Dallas, Texas, zima 1998.**)

6.8 Shadow lozinke

Shadow lozinke način su čuvanja vaših enkriptiranih lozinki nedostupnim običnom korisniku. Obično su te enkriptirane lozinke pohranjene u datoteci `/etc/passwd` gdje ih svi mogu pročitati. Zatim mogu pokrenuti programe za pogađanje lozinke i pokušati ju saznati. Shadow lozinke te informacije pohranjuju u datoteku `/etc/shadow` koju mogu čitati samo privilegirani korisnici. Da bi shadow lozinke funkcionirale, svi vaši programi kojima treba pristup informacijama o lozinci moraju se ponovo kompajlirati kako bi ih podržavali. PAM (već spomenut) vam također omogućava da samo uključite shadow modul i ne zahtijeva ponovno kompajliranje izvršnih datoteka. Ako je to potrebno, za daljne informacije pogledajte **Shadow Password HOWTO**. Dostupan je na `<http://sunsite.unc.edu/LDP/HOWTO/Shadow-Password-HOWTO.html>`. Sada je relativno zastario i nije potreban distribucijama koje podržavaju PAM.

6.9 Crack i John the Ripper

Ako iz nekog razloga vaš passwd program ne sili teško pogodive lozinke, možda ćete htjeti pokrenuti program za razbijanje lozinki i provjeriti da li su lozinke vaših korisnika sigurne.

Programi za razbijanje lozinki zasnovani su na jednostavnoj ideji. Isprobaju svaku riječ u rječniku i zatim njihove varijacije. Svaku enkriptiraju i provjeravaju da li se slaže s vašom enkriptiranom lozinkom. Ako da, unutra su.

Više ih je u divljini... Dva najzapaženija su Crack i John the Ripper `<http://www.false.com/security/john/index.html>`. Zauzet će vam dosta procesorskog vremena, ali bi vam trebali reći da li bi napadač mogao ući koristeći ih, ako ih pokrenete prije njega i obavijestite korisnike sa slabim lozinkama. Primjetite da bi napadač prije toga morao iskoristiti neku drugu rupu da bi dobio vašu passwd (Unixov `/etc/passwd`) datoteku, ali one su češće nego što mislite.

6.10 CFS i TCFS

CFS (Cryptographic File System – kriptografski datotečni sustav) je metoda enkriptiranja cijelog datotečnog sustava koji korisnicima omogućava pohranjivanje enkriptiranih datoteka. Koristi NFS poslužitelj koji radi na lokalnom stroju. RPM-ovi se nalaze na `<http://www.replay.com/redhat/>`, a više informacija o tome kako to sve radi na `<ftp://ftp.research.att.com/dist/mab/>`.

TCFS (Transparent Cryptographic File System – transparentni...) poboljšava CFS, dodavajući više integracije s datotečnim sustavom, tako da je proziran korisnicima koji ga koriste. Više informacija na `<http://edu-gw.dia.unisa.it/tcfs/>`.

6.11 X11, SVGA i sigurnost prikaza

6.11.1 X11

Važno je da osigurate svoj grafički prikaz kako bi spriječili napadače u stvarima kao što je: krađa vaših lozinki dok ih tipkate bez da ste toga svjesni, čitanje dokumenata ili informacija koje čitate na svom ekranu ili čak korištenje rupe za pristup nadkorisnika. Pokretanje X aplikacija preko mreže također može biti igranje s vatrom koje omogućuje njuškalima da gledaju cijelu vašu interakciju s udaljenim sustavom.

X ima više mehanizama za kontrolu pristupa. Najjednostavniji od njih zasniva se na imenu računala. xhost možete koristiti za određivanje računala kojima je dozvoljen pristup vašem prikazu. To uopće nije sigurno. Ako netko ima pristup vašem računalu može koristiti `xhost + svoje računalo` i lako ući. Također, ako dopuštate pristup neprovjerenom stroju, svatko može gledati vaš prikaz.

Ako koristite xdm (**X** **D**isplay **M**anager) za logiranje, imate puno bolju metodu pristupa: MIT-MAGIC-COOKIE-1. Generira se 128-bitni kolačić i sprema u vašu .Xauthority datoteku. Ako želite omogućiti pristup svom prikazu s drugog računala, koristite naredbu xauth i informacije u vašoj .Xauthority datoteci kako bi se samo toj vezi dozvolio pristup. Pročitajte X-na-daljinu mini-KAKO, dostupan na `<http://meta.mioc.hr/X-na-daljinu.html>`.

Možete koristiti i ssh (v. ssh, gore) za sigurne X veze. To ima prednost transparentnosti krajnjem korisniku, a znači da mrežom kolaju samo enkriptirani podaci.

Za više informacija o sigurnosti u X-u pogledajte man stranicu Xauthority. Najsigurnije je koristiti xdm za logiranje na svoju konzolu, a zatim ssh za pokretanje X programa s udaljenih računala.

6.11.2 SVGA

SVGAlib programi obično su SUID-root kako bi mogli pristupiti grafičkoj kartici vašeg Linux sustava. To ih čini vrlo opasnima. Ako se sruše, obično morate ponovo dignuti računalo da bi dobili koristivu konzolu. Provjerite da su SVGA programi koje imate autentični i da im se može barem ponešto vjerovati. Još bolje, nemojte ih uopće imati.

6.11.3 GGI

Linux GGI (**G**eneric **G**raphics **I**nterface – projekt općeg grafičkog sučelja) projekt pokušava rješiti nekoliko problema grafičkih sučelja na Linuxu. GGI će malen dio video koda pomaknuti u kernel, a zatim kontrolirati pristup grafičkom sustavu. To znači da će GGI moći bilo kada dovesti vašu konzolu u dobro stanje. Također će omogućiti sigurne ključeve za upozorenje da na vašoj konzoli ne rade trojanski konji koji se predstavljaju kao login. `<http://synergy.caltech.edu/~ggi/>`

7 Sigurnost kernela

Ovo je opis konfiguracijskih opcija kernela koje se odnose na sigurnost i objašnjene njihove funkcije i korištenja.

Zbog toga što kernel kontrolira mrežni rad vašeg računala, važno je da je on vrlo siguran te da mu se ne može naštetiti. Kako bi spriječili neke od najnovijih mrežnih napada, trebali biste pokušati održati verziju svog kernela svježom. Nove kernele možete naći na `<ftp://ftp.kernel.org/>`.

7.1 Opcije pri kompajliranju kernela

IP: Drop source routed frames (CONFIG_IP_NOSR)

Ova bi opcija trebala biti uključena. Source routed okviri u paketu sadrže cijeli put do svog odredišta. To znači da ruteri kroz koje paket prolazi ne moraju pregledati paket, pa ga samo proslijeđuju. To može dovesti do ulaska podataka u sustav koji možda iskorištavaju sigurnosnu rupu.

IP: Firewalling (CONFIG_IP_FIREWALL)

Ova je opcija potrebna samo ako ćete konfigurirati svoj stroj kao firewall, koristiti masquerading ili želite zaštititi svoju radnu stanicu koja se povezuje modemom od nečijeg ulaženja kroz PPP sučelje.

IP: forwarding/gatewaying (CONFIG_IP_FORWARD)

Ako uključite IP forwarding (prosljeđivanje), vaš Linux sustav u biti postaje ruter. Ako je vaš stroj na mreži, možete proslijeđivati podatke s jedne mreže na drugu, i možda potkopavati firewall koji je postavljen da to spriječi. Normalni dial-up korisnici ovo će isključiti, a ostali bi se korisnici trebali usredotočiti na sigurnosne implikacije. Računala koja su firewalli ovo trebaju uključeno, zajedno sa softverom za firewall.

IP prosljeđivanje možete dinamički uključivati naredbom:

```
root#  echo 1 > /proc/sys/net/ipv4/ip_forward
```

te isključivati naredbom:

```
root#  echo 0 > /proc/sys/net/ipv4/ip_forward
```

Ta datoteka (i mnoge druge datoteke u `/proc`) uvijek će izgledati duge 0 znakova, ali to zapravo nije istina. Ovo je nova opcija kernela, pa provjerite da li koristite verziju 2.0.33 ili noviju.

IP: firewall packet logging (CONFIG_IP_FIREWALL_VERBOSE)

Ova opcija pruža informacije o paketima koje je vaš firewall primio, kao što je pošiljatelj, primatelj, port, itd.

IP: always defragment (CONFIG_IP_ALWAYS_DEFRAG)

Inače je ova opcija isključena, ali ako postavljate firewall ili masquerading, trebat ćete ju uključiti. Kada se podaci šalju od jednog do drugog računala, nisu uvijek poslani u jednom paketu, nego fragmentirani u više komada. Problem s time je što se broj porta pohranjuje samo u prvom fragmentu. To znači da netko može ubaciti informacije u ostale pakete za vašu vezu, koje tamo ne bi smjele biti.

IP: syn cookies (CONFIG_SYN_COOKIES)

SYN napad je DoS (**D**enial **o**f **S**ervice – poricanje usluge) napad koji zauzima sve resurse vašeg računala, zbog čega ga vi morate ponovo dignuti. Nema razloga da ovo u normalnoj situaciji ne uključite.

Packet Signatures (CONFIG_NCPFS_PACKET_SIGNING)

Ovo je opcija iz 2.1 serije kernela koja će za veću sigurnost potpisivati NCP pakete. Obično je možete ugasiti, ali tu je ako vam je potrebna.

IP: Firewall packet netlink device (CONFIG_IP_FIREWALL_NETLINK)

Ovo je stvarno zgodna opcija koja vam omogućava analizu prvih 128 bajtova paketa iz programa u korisničkom prostoru, kako bi odlučili da li ćete primiti ili odbaciti paket na osnovu njegove valjanosti.

7.2 Kernel uređaji

Na Linuxu će vam u osiguranju pomoći i nekoliko blok i znakovnih uređaja.

Kroz dva uređaja `/dev/random` i `/dev/urandom` kernel stalno daje slučajne podatke.

I `/dev/random` i `/dev/urandom` bi trebali biti dovoljno sigurni za korištenje u generiranju PGP ključeva, SSH izazova i drugim primjenama gdje su potrebni sigurni, slučajni brojevi. Napadači ne bi smjeli moći predvidjeti slijedeći broj na temelju bilo kojeg početnog niza brojeva iz tih izvora. Uloženo je mnogo napora u osiguravanju da su brojevi koje dobijete odatle slučajni u svakom smislu riječi slučajni.

Jedina je razlika što `/dev/random`-u ponestane brojeva i pa morate čekati da ih se više nakupi. No, na nekim sustavima, može dugo čekati na novi ulaz korisničkih podataka u sustav. Zato prije korištenja `/dev/random` morate biti pažljivi. (Možda je najbolje rješenje reći korisniku da udara po tipkovnici dok mu ne kažete "U redu, dosta je" dok generirate osjetljive ključeve.)

`/dev/random` pruža vrlo kvalitetnu entropiju, generiranu mjerenjem vremena između interruptova i slično. Ako nema dovoljno komada slučajnih podataka, blokira se.

/dev/urandom je sličan, ali kada je zaliha entropije mala, dat će vam kriptografski jaku izmjenu onoga što ima. To nije sigurno, ali je dovoljno većini aplikacija.

Možda ćete čitati iz tih uređaja koristeći nešto kao:

```
root#  head -c 6 /dev/urandom | uuencode -
```

To će na konzoli ispisati šest slučajnih znakova prikladnih za generiranje lozinke.

Za opis algoritma pogledajte /usr/src/linux/drivers/char/random.c.

Hvala Theodoreu Y. Ts'ou, Jonu Lewisu i drugima s Linux-kernel mailing liste što su mi (Daveu) pomogli s ovim.

8 Sigurnost mreže

Sigurnost mreže postaje sve više važna jer ljudi na njoj provode sve više vremena. Kompromitiranje sigurnosti mreže često je puno lakše nego kompromitiranje lokalne ili fizičke sigurnosti, te puno češće.

Ima više dobrih alata koji će vam pomoći u osiguravanju mreže, a sve više ih se isporučuje s Linux distribucijama.

8.1 Sniferi paketa

Jedan od najčešćih načina na koji uljez dobiva pristup više računala na vašoj mreži je pokretanjem snifera paketa na već osvojenom računalu. Taj "snifer" samo na Ethernet portu sluša stvari kao što je "Password", "Login" i "su" u toku paketa i zatim promet koji slijedi zapisuje. Na taj način napadač dobiva lozinke za sustave u koje nije ni pokušao provaliti. Lozinke u čistom tekstu osobito su ranjive na takav napad.

PRIMJER: računalo A je kompromitirano. Napadač instalira snifer. Snifer zapazi administratora koji se logira u računalo B s računala C. Dobiva osobnu lozinku administratora dok se logira na B. Zatim administrator pokreće su da bi riješio neki problem. Sada napadač ima lozinku za računalo B. Napon toga administrator nekome dopušta da se s njegovog računa logira na računalo Z na nekoj drugoj mreži. Sada napadač ima login/lozinku za računalo Z.

U današnja vremena napadač više ne mora ni kompromitirati računalo da bi to izveo, može jednostavno donijeti i laptop ili PC u zgradu i prikvačiti se na vašu mrežu.

Korištenje ssh ili drugih metoda enkriptiranja lozinki onemogućava ovaj napad. Stvari kao što je APOP za POP račune također ga sprečavaju. (Obični POP logini vrlo su ranjivi na njega, kao i sve ostalo što preko veze šalje čitljive lozinke.)

8.2 Usluge sustava i tcp_wrapperi

Čim svoj Linux sustav stavite na *bilo koju* mrežu, prvo morate pogledati koje usluge trebate ponuditi. Usluge koje ne morate nuditi treba isključiti tako da se brinete o jednoj stvari manje, a napadači imaju manje mjesta za iskorištavanje rupa.

Pod Linuxom ima više načina za isključivanje usluga. Možete pogledati svoju /etc/inetd.conf datoteku i vidjeti koje usluge nudi inetd. Isključite one nepotrebne komentiranjem (stavite # na početku reda), a zatim svom inetd procesu pošaljite SIGHUP.

Također možete obrisati (ili zakomentirati) usluge u svojoj /etc/services datoteci. To znači da lokalni klijenti također neće moći naći uslugu (tj., ako maknete FTP i pokušate FTP-ati drugo računalo sa svoga, dobit ćete poruku "usluga nepoznata"). Obično nema potrebe brisati usluge jer time ne dobivate nikakvo dodatno osiguranje. Ako lokalni korisnik želi koristiti FTP čak i ako ste ga zakomentirali, mogu samo reći svom klijentu da koristi standardni FTP port i raditi potpuno normalno.

Neke od usluga koje ćete željeti ostaviti su:

- FTP
- telnet
- mail, kao što je POP3 ili IMAP
- identd
- time (vrijeme)

Ako znate da određeni paket uopće nećete koristiti, možete ga i u potpunosti obrisati. `rpm -e` na distribuciji Red Hat obrisat će cijeli paket. Na Debianu `dpkg` vjerojatno obavlja isti posao.

Zatim, stvarno ćete željeti isključiti rsh/rlogin/rcp programe, kao i pokretanje logina (koristi ga rlogin), shella (koristi ga rcp) i execa (koristi ga rsh) u `/etc/inetd.conf`. Ti su protokoli iznimno nesigurni i bili su uzrok mnogih rupa.

Trebate provjeriti svoj `/etc/rc.d/rcB.d`, gdje je B run level vašeg sustava da vidite da li se u tom direktoriju pokreću poslužitelji koji nisu potrebni. Datoteke u `/etc/rc.d/rcB.d` zapravo su simboličke veze na direktorij `/etc/rc.d/init.d`. Ako preimenujete datoteku u direktoriju `init.d`, prestat će vrijediti sve simboličke veze iz `/etc/rc.d/rcB.d`. Ako želite isključiti uslugu samo za određeni run level, odgovarajućoj datoteci u ime stavite malo `s` umjesto velikog `S`, kao što je `S45dhcpd`.

Ako imate rc datoteke u BSD stilu, programe koji vam nisu potrebni potražite u `/etc/rc*`.

Većina distribucija Linuxa isporučuje se s tcp_wrapperi, koji "zamataju" sve vaše TCP usluge. inetd poziva tcp_wrapper (tcpd) umjesto pravog poslužitelja. Zatim tcpd provjerava računalo koje zahtijeva uslugu i poziva pravi poslužitelj ili odbija pristup tome računalu. tcpd vam omogućava ograničavanje pristupa vašim TCP uslugama. Trebali biste napraviti `/etc/hosts.allow` i dodati samo ona računala kojima je potreban pristup uslugama vašeg stroja.

Ako ste kućni korisnik s modemskom vezom, predlažemo vam odbijanje pristupa svima. tcpd također logira neuspješne pokušaje pristupa uslugama, tako da saznate kad ste pod napadom. Ako dodate nove usluge, konfigurirajte ih tako da za TCP koriste tcp_wrapper. Na primjer, obični korisnik s modemskom vezom može spriječiti spajanje drugih na njegov stroj zadržavajući pritom mogućnost skidanja pošte i uspostavljanja veza na Internet. Ako to želite, možete dodati ove redove svojem `/etc/hosts.allow`:

```
ALL: 127
```

I, naravno, `/etc/hosts.deny` bi ovako izgledao:

```
ALL: ALL
```

što će spriječiti vanjska spajanja na vaše računalo, ali ostaviti mogućnost unutarnjeg povezivanja na poslužitelje na Internetu.

8.3 Provjerite svoje DNS-ove

Održavanje DNS informacija o svim strojevima na vašoj mreži svježim može pomoći u povećavanju sigurnosti. U slučaju povezivanja neodobrenog stroja na vašu mrežu lako ćete ga prepoznati po nedostatku DNS zapisa. Mnoge se usluge mogu konfigurirati da ne prihvaćaju veze s računala koje nemaju valjane DNS zapise.

8.4 identd

identd je malen program koji obično pokreće inetd. On vodi računa o tome koji korisnik koristi koju TCP uslugu, a zatim to prijavljuje onima koji to traže.

Mnogi ljudi ne razumiju korisnost identda, pa ga isključuju ili blokiraju sve vanjske zahtijeve za njega. identd nije tu da pomogne udaljenim računalima. Nema načina na koji možete saznati da li su podaci koje ste dobili od udaljenog identda točni ili ne. U identd zahtjevima nema autentifikacije.

Zašto bi ga onda pokrenuli? Jer pomaže *vama* i još je jedna ispomoć u praćenju. Ako vaš identd nije kompromitiran, onda znate da udaljenim računalima govori korisničko ime ili UID ljudi koji koriste TCP usluge. Ako se administrator udaljenog stroja obrati vama i kaže da je taj i taj korisnik pokušavao upasti na njihov stroj, lako možete poduzeti mjere protiv tog korisnika. Ako nemate identd, morat ćete proći kroz puno puno logova, saznati tko je bio logiran u to vrijeme, te općenito izgubiti puno više vremena za pronalaženje korisnika.

identd koji se isporučuje s većinom distribucija konfigurabilniji je nego što mnogi misle. Za određene korisnike ga možete ugasiti (mogu napraviti datoteku `.noidentd`), možete bilježiti sve identd zahtjeve (preporučam), čak ga možete natjerati da vrati UID umjesto korisničkog imena, ili čak NO-USER.

8.5 SATAN, ISS i drugi mrežni skeneri

Postoji više raznih softverskih paketa za skeniranje strojeva i mreža na osnovu portova i usluga. SATAN i ISS dva su poznatija. Oni se povežu s ciljnim računalom (ili svim takvim na mreži) na svim mogućim portovima, pokušavajući saznati koje se tamo nude usluge. Na osnovu tih informacija možete naći računalo ranjivo na određenu rupu na poslužitelju.

SATAN (**S**ecurity **A**dministrator's **T**ool for **A**nalyzing **N**etworks – alat sigurnosnog administratora za analizu mreža) je port skener s WWW sučeljem. Može se konfigurirati za laganu, srednju ili temeljitu provjeru na računalu ili mreži računala. Pametno je nabaviti SATAN i skenirati svoje računalo ili mrežu i popraviti pronađene probleme. Budite sigurni da ste SATAN dobili sa `sunsitea` ili uglednog FTP ili WWW poslužitelja. Preko mreže se distribuirala trojanska kopija SATAN-a. `<http://www.trouble.org/~zen/satan/satan.html>`

ISS (**I**nternet **S**ecurity **S**canner) je još jedan port skener. Brži je od SATAN-a i zbog toga bolji za veće mreže. Međutim, SATAN pruža više detalja.

Abacus-Sentry je komercijalni port skener s `www.psionic.com`. Pogledajte njegovu WWW stranicu za više informacija: `<http://www.psionic.com>`.

Otkrivanje port skenera

Postoje neki alati koji će vas uzbuniti tokom testiranja SATAN-om, ISS-om ili drugim programima za skeniranje. No, slobodno korištenje tcp_wrappera i redovito provjeravanje logova dat će isti rezultat. Čak i pri najslabijoj jačini SATAN ostavlja tragove u log datotekama na standardnom Red Hat sustavu.

8.6 sendmail, qmail i MTA-ovi

Jedna od najvažnijih usluga koju možete ponuditi je poslužitelj pošte. Nažalost, to je i jedna od najranjivijih, zbog broja zadataka koje obavlja i privilegija koje obično treba.

Ako koristite sendmail, vrlo je važno održavati verziju svježom. sendmail ima dugu, dugu povijest sigurnosnih rupa. Uvijek budite sigurni da imate najnoviju verziju. `<http://www.sendmail.org/>`

Ako vam je dosta nadograđivanja sendmaila svaki tjedan, možete se prebaciti na qmail. qmail je ispočetka oblikovan s pažnjom na sigurnost. Brz je, stabilan i siguran. `<http://www.qmail.org>`

8.7 Denial of Service (poricanje usluga) napadi

Kod Denial of Service napada napadač pokušava neki resurs zauzeti toliko da on nije u stanju odgovarati na dobre zahtjeve, odnosno uskratiti dobrim korisnicima pristup vašem stroju.

Broj takvih napada u zadnjih je nekoliko godina vrlo porastao. Neki od najpopularnijih i najnovijih navedeni su dolje. Međutim, novi se stalno pojavljuju, pa je ovo samo nekoliko primjera. Za svježije informacije čitajte Linux liste o sigurnosti i bugtraq listu i arhive.

SYN flooding

SYN flooding (SYN "poplava") je mrežni DoS napad. Iskorištava "kruženje" u načinu na koji se stvaraju TCP veze. Noviji Linux kerneli (2.0.30 i više) imaju nekoliko konfigurabilnih opcija za sprečavanje SYN flood napada koji ljudima onemogućavaju pristup vašem računalu ili uslugama. Za pravilnu zaštitu u kernelu pogledajte dio o sigurnosti kernela.

Pentium F00F greška

Nedavno je otkriveno da niz asembliranih naredbi poslan pravom Intel Pentium procesuru resetira računalo. To vrijedi za svaki stroj s Pentium procesorom (ne klonovima, niti Pentiumom Pro ili PII), bez obzira na koji operacijski sustav koristi. Linux kernel 2.0.32 i bolji sadrže zaobilaznicu za ovu grešku koja sprečava rušenje računala. Kernel 2.0.33 ima bolju verziju rješenja i preporuča se prije 2.0.32. Ako radite na Pentiumu, odmah se nadogradite!

Ping flooding

Ping flooding je jednostavan DoS napad grubom silom. Napadač vašem računalu šalje "poplavu" ICMP paketa. Ako to rade s računala s boljom propusnošću mreže od vašeg, vaše neće moći poslati ništa na mrežu. Varijacija ovog napada, zvana **smurfing** vašem stroju šalje ICMP pakete s povratnom adresom *vašeg* stroja, tako ih je teže otkriti. Više informacija o smurf napadu možete naći na `<http://www.quadrunner.com/~chuegen/smurf.txt>`.

Ako ikada budete pod ping flood napadom, koristite alat kao što je tcpdump kako bi otkrili odakle paketi dolaze (ili se čini da dolaze), a zatim s tim informacijama kontaktirajte svog ISP-a. Ping floodovi najlakše se zaustavljaju na razini rutera ili korištenjem firewalla.

Ping o' Death

Ping o' Death napad rezultat je dolazećih **ICMP ECHO REQUEST** paketa većih od onog što može podnijeti kernel struktura za pohranjivanje tih podataka. Zbog toga što slanje jednog velikog (65 510 bajtova) ping paketa mnogim sustavima uzrokuje njihovo rušenje ovaj je problem ubrzo rješen i više se o njemu ne treba brinuti.

Teardrop/New Tear

Jedan od najnovijih napada koji iskorištava grešku u kodu za IP fragmentaciju na Linuxu i Windowsima. Rješen je u verziji kernela 2.0.33 i ne zahtijeva odabiranje bilo koje opcije pri kompajliranju kernela. Čini se da Linux nije ranjiv na newtear napad.

Većinu koda koji iskorištava rupe i detaljnije informacije kako rade možete naći na `<http://www.rootshell.com>` korištenjem pretraživanja.

8.8 Sigurnost NFS-a

NFS (**N**etwork **F**ile **S**ystem – mrežni datotečni sustav) je vrlo rasprostranjen protokol za dijeljenje datoteka. Omogućava poslužiteljima na kojima radi nfsd i mountd da "izvoze" cijele datotečne sustave drugim strojevima koji imaju podršku za NFS u svojim kernelima (ili drukčiju podršku ako to nisu Linuxi). mountd vodi račune o montiranim datotečnim sustavima u `/etc/mtab` i može ih pokazati preko naredbe `showmount`.

Mnogi sustavi koriste NFS za posluživanje home direktorija korisnicima, tako da nije važno s kojeg se stroja u tom dijelu logiraju jer će uvijek imati svoje datoteke.

U izvoženju datotečnih sustava moguć je manji stupanj "sigurnosti". Možete natjerati nfsd da mapira vanjskog root korisnika (UID=0) na nobody (nitko) korisnika, onemogućavajući im potpun pristup datotekama koje se izvoze. Međutim, pošto pojedini korisnici imaju svoj pristup (ili barem isti UID) datotekama, udaljeni se nadkorisnik može logirati ili su-ati na njihov račun i imati potpun pristup datotekama. To je samo mala smetnja napadaču koji ima pristup montiranju vaših udaljenih datotečnih sustava.

Ako baš morate koristiti NFS, provjerite da li izvozite samo onim strojevima kojima je to nužno. Nikad ne izvozite cijeli svoj root direktorij, izvozite samo potrebne direktorije.

Za više informacija o NFS-u pročitajte **NFS HOWTO**: `<http://sunsite.unc.edu/mdw/HOWTO/NFS-HOWTO.html>`.

8.9 NIS (bivši YP)

NIS (**N**etwork **I**nformation **S**ervices – mrežna informativna usluga, bivši YP) je sredstvo distribuiranja informacija skupini računala. NIS master sadrži informacijske tabele koje pretvara u NIS map datoteke. Te se mape onda nude preko mreže omogućavajući NIS klijent strojevima dobivanje informacija o loginu, lozinki, home direktoriju i ljusci (sve informacije iz standardnog `/etc/passwd`). To korisnicima omogućava mijenjanje lozinke jednom, koje zahvaća sve stroje u NIS domeni.

NIS uopće nije siguran. To nikad nije ni trebao biti. Trebao je biti jednostavan i koristan. Svatko tko može pogoditi ime vaše NIS domene (bilo gdje na mreži) može dobiti primjerak vaše `passwd` datoteke i koristiti Crack i John the Ripper na lozinkama vaših korisnika. Moguće je i prisluškivanje NIS-a i mnoge vrste prljavih trikova. Ako morate koristiti NIS, budite barem svjesni opasnosti.

Postoji puno sigurnija zamjena za NIS, NIS+. Za više informacija pogledajte **NIS HOWTO**: `<http://sunsite.unc.edu/mdw/HOWTO/NIS-HOWTO.html>`.

8.10 Firewallovi

Firewallovi su sredstvo ograničavanja protoka informacija u i iz vaše lokalne mreže. Obično je firewall stroj spojen i na Internet i na vaš LAN, tako da se Internetu iz vašeg LAN-a može pristupiti samo kroz njega. Na taj način firewall kontrolira što prolazi vezom između Interneta i vašeg LAN-a.

Postoji više vrsta i načina postavljanja firewalla. Linux strojevi prilično su dobri i jeftini firewallovi. Kod za firewall može se ugraditi ravno u 2.0 i bolje kernele. ipfwadm, alat u korisničkom prostoru, omogućava vam mijenjanje u letu tipova mrežnog prometa koje propuštate. Određene vrste mrežnog prometa možete i logirati.

Firewallovi su vrlo korisna i važna tehnika osiguravanja vaše mreže. Važno je da shvatite kako nikad ne smijete misliti da, samo zato što imate firewall, ne trebate sigurne strojeve iza njega. To je smrtna greška. Pogledajte vrlo dobar **Firewall HOWTO** na svojoj najsvježijoj `sunsite` arhivi za više informacija o firewallima pod Linuxom. `<http://sunsite.unc.edu/mdw/HOWTO/Firewall-HOWTO.html>`

Više informacija također se može naći u **IP-Masquerade mini-HOWTO**: `<http://sunsite.unc.edu/mdw/HOWTO/mini/IP-Masquerade.html>`-

Više informacija o ipfwadmu (alatu kojim možete mijenjati opcije svog firewalla) može se naći na njegovoj WWW stranici: `<http://www.xos.nl/linux/ipfwadm/>`.

9 Sigurnosne pripreme (prije nego se uključite u mrežu)

Dakle, provjerili ste svoj sustav, odlučili da je dovoljno siguran i spremni ste ga uključiti u mrežu. Nekoliko je stvari koje bi sada trebali obaviti kako bi bili spremni u slučaju da se upad stvarno dogodi, tako da uljeza brzo možete onemogućiti i oporaviti se te nastaviti rad.

9.1 Napravite potpun backup svoga stroja

Rasprava o metodama backupa i pohranjivanja izvan je dosega ovog dokumenta, ali nekoliko riječi vezanih uz backup i sigurnost:

Ako na particiji imate manje od 650 MB podataka, CD-R kopiranje podataka je dobra metoda (jer je s njime teško kasnije petljati, a ako se pravilno pohrani može trajati dugo vremena). Trake i druge medije na koje se ponovo može pisati treba zaštiti od pisanja čim je vaš backup potpun i provjeren za sprečavanje petljanja. Osigurajte da su vaši backupi pohranjeni u sigurnom području isključenom iz mreža. Dobar backup osigurava dobru početnu točku za vraćanje sustava u normalno stanje.

9.2 Izbor dobrog rasporeda backupa

Ciklus od šest traka lako je održavati. To se odnosi na četiri vrpce tijekom tjedna, jednu za parne petke i jednu za neparne petke. Svaki dan obavljajte inkrementalni backup, a svaki petak potpuni. Ako napravite određene promjene ili sustavu dodate važne podatke, backup će vam dobro doći.

9.3 Backupirajte svoju RPM ili Debian bazu podataka datoteka

U slučaju provale možete iskoristiti svoju RPM bazu podataka datoteka kao što koristite Tripwire, ali samo ako ste sigurni da nije mijenjana. Kopirajte RPM bazu na disketu i stalno ju držite izvan mreže. Debian distribucija vjerojatno ima nešto slično.

Točnije, datoteke `/var/lib/rpm/fileindex.rpm` i `/var/lib/rpm/packages.rpm` najvjerojatnije neće stati na jednu disketu. Sažete bi trebale stati svaka na svoju.

Sada, ako je vaš sustav kompromitiran, možete koristiti naredbu:

```
root#  rpm -Va
```

za provjeru svake datoteke na sustavu. Pogledajte man stranicu RPM-a – postoje neke opcije za manje poruka.

To znači da će se, svaki put kada se sustavu doda novi RPM, RPM baza morati ponovo arhivirati. Vi odlučite što vam je draže – prednosti ili nedostaci.

9.4 Praćenje logova vašeg sustava

Vrlo je važno da informacije koje dolaze od sysloga nisu kompromitirane. Dati dozvole za čitanje i pisanje u `/var/log` samo ograničenom broju korisnika dobar je početak.

Svakako pratite što se tamo bilježi, posebno za **auth**. Višestruki neuspješni logini, na primjer, mogu značiti pokušaj provale.

Gdje ćete naći log datoteke ovisi o vašoj distribuciji. Na Linux sustavu koji slijedi **Linux Filesystem Standard**, kao što je Red Hat, potražit ćete ih u `/var/log` i tamo provjeravati `messages`, `mail.log` i druge.

Gdje vaša distribucija logira stvari saznat ćete u svojoj `/etc/syslog.conf` datoteci. To je datoteka koja govori syslogd-u (demonu za logiranje sustava) gdje da logira razne poruke.

Također ćete možda htjeti konfigurirati svoju skriptu ili demon za rotiranje logova, tako da logovi traju dulje i da imate više vremena za njihovo pregledavanje. Na novijim distribucijama Red Hata pogledajte paket logrotate. Druge distribucije vjerojatno imaju sličan proces.

Ako je s vašim logovima netko petljao, pokušajte saznati kada je petljanje počelo i s čim je sve izgleda petljano. Postoje li dugi periodi vremena za koje nema podataka? Dobra je ideja provjeriti backup traka (ako ih imate) za izvorne log datoteke.

Uljez obično mijenja logove kako bi prikrio tragove, ali svejedno ih treba provjeravati za čudne stvari. Možda primjetite kako je uljez pokušavao ući ili iskoristiti sigurnosnu rupu kako bi dobio rootov račun. Možda vidite logove prije nego što ih uljez stigne izmjeniti.

Trebali biste odvojiti auth od drugih logova, kao što su pokušaji korištenja `su` za zamjenu korisnika, pokušaje logina i druge informacije o korisnicima.

Ako je to moguće, konfigurirajte syslog da šalje kopije svih najvažnijih podataka na siguran sustav. To će spriječiti uljeza u prikrivanju tragova preko brisanja svojih pokušaja logina/su-a/FTP-a/itd. Pogledajte man stranicu syslog.conf i opciju @.

Na kraju, log datoteke su mnogo nekorisnije kada ih nitko ne čita. Oduzmite si malo vremena svako malo i pogledajte svoje logove, te probajte shvatiti kako izgleda običan dan. To će vam pomoći u uočavanju neobičnih stvari.

9.5 Primjenite sve nove nadogradnje sustava

Većina korisnika Linuxa instalira s CD-ROM-a. Zbog brzog ritma sigurnosnih ispravaka, stalno izlaze novi (ispravljeni) programi. Prije nego što se povežete s mrežom, pametno je provjeriti FTP poslužitelj svoje distribucije (na primjer *ftp.redhat.com*) i nabaviti sve novije pakete otkad ste primili CD-ROM distribucije. Često takvi paketi sadrže važne sigurnosne ispravke, pa je pametno instalirati ih.

10 Što učiniti tokom i nakon provale

Dakle, jeste li slijedili neke od ovih (ili drugih) savjeta i otkrili provalu? Najprije trebate ostati staloženi. Panični postupci mogu uzrokovati više štete od napadača.

10.1 Narušavanje sigurnosti upravo se odvija

Uočavanje narušavanja sigurnosti koje se upravo odvija može biti napeto. Vaša reakcija imat će velike posljedice.

Ako je narušavanje kojeg gledate fizičko, vjerojatno ste uočili nekoga tko je provalio u vaš dom, ured ili laboratorij. Trebate obavijestiti lokalne vlasti. U laboratoriju ste možda vidjeli kako netko pokušava otvoriti kućište ili resetirati stroj. Ovisno o vašem autoritetu i postupcima, možete ih zamoliti da prestanu ili pozvati svoje lokalno osiguranje.

Ako ste uočili lokalnog korisnika koji pokušava narušiti vašu sigurnost, prvo trebate potvrditi da je on stvarno onaj za kojeg mislite da je on. Provjerite odakle se logirao. Je li to računalo s kojeg se i normalno logiraju? Ne? Onda ga kontaktirajte neelektronskim sredstvima. Na primjer, pozovite ih telefonom ili odšetajte do njihovog ureda/doma i razgovarajte s njima. Ako kažu da su logirani, možete ih zatražiti da objasne što su radili ili da to prestanu raditi. Ako nisu i nemaju blage veze o čemu govorite, taj događaj vjerojatno zahtjeva dodatnu istragu. Pazite na takve događaje i skupite puno informacija prije nego nekoga optužite.

Ako ste otkrili mrežnom narušavanje, najprije (ako možete) isključite mrežu. Ako su spojeni modemom, isključite kabel modema, a ako su spojeni Ethernetom, isključite kabel Etherneta. To će ih spriječiti u daljnjem nanošenju štete, a vjerojatno će to shvatiti kao problem u mreži, a ne razotkrivanje.

Ako ne možete isključiti mrežu (imate vrlo zaposlen poslužitelj ili nemate fizičku kontrolu nad svojim računalima), slijedeći najbolji korak je onemogućavanje veza s uljezovog računala pomoću tcp_wrappera ili ipfwadma.

Ako ne možete isključiti sve ljude sa stroja na kojem je uljez, morat ćete se zadovoljiti isključivanjem korisničkog računa. Primjetite da to nije jednostavno. Morate paziti na `.rhosts` datoteke, FTP pristup i hrpu stražnjih vrata).

Nakon što ste učinili nešto od navedenog (isključili mrežu, onemogućili pristup sa njegovog računala i/ili isključili njegov račun), morate mu ubiti sve procese i odlogirati ih.

Slijedećih nekoliko minuta morate pažljivo gledati na svoj stroj jer će napadač pokušati ući ponovno. Možda će koristiti drugi račun i/ili mrežnu adresu.

10.2 Narušavanje sigurnosti već se dogodilo

Uočili ste narušavanje koje se već dogodilo ili ste ga uočili i isključili (još bolje) napadača iz sustava. Što sad?

10.2.1 Zatvaranje rupe

Ako možete otkriti način na koji je napadač ušao u vaš sustav, pokušajte zatvoriti rupu. Na primjer, možda vidite nekoliko zapisa o FTP-u baš prije nego što se korisnik logirao. Isključite FTP uslugu i provjerite da li postoji novija verzija ili neka od listi zna rješenje.

Provjerite sve svoje log datoteke i pogledajte da li na vašim listama i stranicama o sigurnosti ima novih rupa koje možete ispraviti. Calderine sigurnosne ispravke možete naći na `<http://www.caldera.com/tech-ref/security/>`. Red Hat još nije odvojio sigurnosne ispravke od ispravaka grešaka, no ispravci za njihovu distribuciju nalaze se na `<http://www.redhat.com/errata>`. Vrlo je vjerojatno da će, ako je jedna tvrtka izdala sigurnosnu ispravku, to ubrzo učiniti i ostale.

Ako ne izbacite napadača, vjerojatno će se vratiti. Ne samo na vaše računalo, nego negdje na vašu mrežu. Ako je pokrenuo snifer paketa, velike su šanse da ima pristup drugim lokalnim strojevima.

10.2.2 Procjenjivanje štete

Najprije procjenite štetu. Što je narušeno? Ako imate provjeru cjelovitosti kao što je Tripwire, pokrenite ju i ona će vam reći. Ako ne, morat ćete sami pogledati sve svoje najvažnije podatke.

Pošto je Linux sustave sve lakše i lakše instalirati, možete svoje konfiguracijske snimiti na sigurno, obrisati svoj disk/ove i ponovno instalirati, a zatim vratiti korisničke datoteke iz backupa i konfiguracijske datoteke. To će osigurati nov, čist sustav. Ako morate spašavati datoteke s kompromitiranog sustava, budite posebno pažljivi s programima koje vratite jer to mogu biti trojanski konji koje je postavio uljez.

10.2.3 Backup, backup, backup!

Redovit backup dar je s neba za sigurnosne probleme. Ako je vaš sustav kompromitiran, potrebne podatke možete vratiti s backupa. Naravno, neki podaci su vrijedni i napadaču, i on će ga ne samo uništiti, već i ukrasti i imati svoje kopije, ali barem ćete još uvijek imati podatke.

Provjerite nekoliko prošlih backupa prije nego vratite datoteku s kojom je petljano. Uljez je možda kompromitirao vaše datoteke prije puno vremena, a vi ste mogli napraviti mnogo uspješnih backupa kompromitirane datoteke!

Narvno, mnoštvo je sigurnosnih briga s backupima. Potrudite se da su na sigurnom mjestu. Budite svjesni tko im ima pristup. (Ako napadač može doći do vaših backupa, ima pristup do svih vaših podataka, a da vi toga niste ni svjesni.)

10.2.4 Pronalaženje uljeza

U redu, izbacili ste uljeza i sredili sustav, ali još niste gotovi. Iako će vjerojatno većina uljeza ostati neuhvaćena, trebate prijaviti napad.

Napad prijavite administratoru sustava s kojeg je napadač napao vaš sustav. Možete ga naći pomoću `whois` ili internicove baze podataka. Možete mu poslati e-mail sa svim primjenjivim zapisima u logu i datumima i vremenima. Ako ste uočili još nešto posebno za svog uljeza, spomenite i to. Nakon što ste poslali e-mail, trebali biste ga (ako ste toliko zapeli) i nazvati telefonom. Ako taj administrator uoči vašeg napadača, onda on može kontaktirati administratora sustava odakle je došao i tako dalje.

Dobri hakeri često koriste mnogo posrednih sustava. Neki (ili mnogi) od njih možda ni ne znaju da su napadnuti. Pokušati doći do krekerovog početnog sustava može biti teško. Ljubaznim ponašanjem prema administratorima od njih možete dobiti puno pomoći.

Također biste trebali obavijestiti sigurnosne organizacije kojih ste dio (CERT ili slično).

11 Izvori informacija o sigurnosti

Tamo vani ima *puno* dobrih stranica o sigurnosti UNIX-a općenito i specifično Linuxa. Vrlo je važno da se pretplatite na jednu (ili više) sigurnosnih mailing listi i pratite sigurnosne ispravke. Većina takvih listi ima vrlo malo prometa i vrlo su informativne.

11.1 FTP poslužitelji

CERT je **C**omputer **E**mergency **R**esponse **T**eam (skupina za hitnu računalnu pomoć). Često šalju uzbune o trenutnim napadima uz ispravke. `<ftp://ftp.cert.org/>`

Replay ima arhive mnogih programa za sigurnost. Pošto su izvan SAD-a, ne moraju poštovati američka kriptografska ograničenja. `<ftp://ftp.replay.com/>`

Matt Blaze je autor CFS-a i sjajan promicatelj sigurnosti. `<ftp://ftp.research.att.com/pub/mab/>`

tue.nl je odličan sigurnosni FTP server u Nizozemskoj. `<ftp://ftp.win.tue.nl/pub/security/>`

11.2 WWW stranice

The Hacker FAQ je FAQ o hakerima: `<http://www.solon.com/~seebs/faqs/hacker.html>`

COAST arhiva ima velik broj Unix sigurnosnih programa i informacija: `<http://www.cs.purdue.edu/coast/>`

Rootshell.com su odlične stranice za traženje rupa koje trenutno krekeri koriste: `<http://www.rootshell.com/>`

BUGTRAQ objavljuje savjete o sigurnosnim problemima: `<http://www.netspace.org/lsv-archive/bugtraq.html>`

CERT, **C**omputer **E**mergency **R**esponse **T**eam (skupina za hitnu računalnu pomoć), objavljuje savjete o čestim napadima na Unix platforme: `<http://www.cert.org/>`

Dan Farmer je autor SATAN-a i mnogih drugih sigurnosnih alata, a njegove stranice imaju neke zanimljive ankete o sigurnosti kao i sigurnosne alate: `<http://www.trouble.org>`

The Linux security WWW dobre su stranice za informacije o sigurnosti Linuxa: `<http://www.aoy.com/Linux/Security/>`

Reptile na svojim stranicama ima dosta dobrih informacija o Linux sigurnosti: `<http://207.237.120.45/linux/>`

Infilsec ima engine za ranjivosti koji vam kaže na što je ranjiva vaša platforma: `<http://www.infilsec.com/vulnerabilities/>`

CIAC redovito objavljuje sigurnosne biltene o čestim rupama: `<http://ciac.llnl.gov/cgi-bin/index/bulletins>`

Dobra početna točka za Linux Pluggable Authentication Modules (uključivi moduli za autentifikaciju) može se naći na `<http://www.kernel.org/pub/linux/libs/pam/>`.

11.3 Mailing liste

BUGTRAQ: za pretplatu na BUGTRAQ pošaljite poruku na *listserv@netspace.org* s retkom `subscribe bugtraq` u tijelu poruke. (Za arhive pogledajte gore navedeno.)

CIAC: pošaljite poruku na *majordomo@tholia.llnl.gov*. U *tijelu* (ne Subject:-u) poruke stavite (jedno ili drugo ili oboje) `subscribe ciac-bulletin`.

11.4 Knjige – tiskani materijali za čitanje

Postoji više dobrih knjiga o sigurnosti. Ovaj dio navest će ih nekoliko. Uz knjige specifično o sigurnosti, sigurnost je pokrivena i u dosta drugih knjiga o administriranju sustava.

D. Brent Chapman i Elizabeth D. Zwicky: **Building Internet Firewalls**
1. izdanje, rujan 1995.
ISBN: 1-56592-124-0

Simson Garfinkel i Gene Spafford: **Practical UNIX & Internet Security**
2. izdanje, travanj 1996.
ISBN: 1-56592-148-8

Deborah Russell i G.T. Gangemi, Sr.: **Computer Security Basics**
1. izdanje, srpanj 1991.
ISBN: 0-937175-71-4

Olaf Kirch: **Linux Network Administrator's Guide**
1. izdanje, siječanj 1995.
ISBN: 1-56592-087-2

Simson Garfinkel: **PGP: Pretty Good Privacy**
1. izdanje, prosinac 1994.
ISBN: 1-56592-098-8

David Icove, Karl Seger i William VonStorch (savjetodavni urednik Eugene H. Spafford): **Computer Crime A Crimefighter's Handbook**
1. izdanje, kolovoz 1995.
ISBN: 1-56592-086-4

12 Rječnik

Host

Računalni sustav povezan na mrežu. (računalo, sustav)

Firewall

Komponenta ili skup komponenti koje ograničavaju pristup između zaštićene mreže i Interneta ili između drugih skupina mreža.

Bastion host

Računalni sustav koji mora biti vrlo osiguran jer je ranjiv na napade, obično zato što je izložen Internetu i glavna točka kontakta korisnika internih mreža. Ime je dobio po vrlo utvrđenim građevinama na vanjskim zidovima srednjevjekovnih dvoraca. Bastioni nadgledaju kritična područja obrane, obično uz jake zidove, prostor za dodatne trupe i ponekad korisne lonce pune kipućeg ulja za obeshrabrivanje napadača.

Dual-homed host

Opće namjenski računalni sustav koji ima barem dva mrežna sučelja.

Packet

Osnovna jedinica komunikacije na Internetu. (paket)

Packet filtering

Radnja koju obavlja uređaj kako bi selektivno kontrolirao tok podataka u i iz mreže. Filtri paketa odobravaju ili blokiraju pakete, obično tokom njihovog usmjeravanja iz jedne u drugu mrežu (najčešće iz Interneta u internu mrežu i obratno). Da bi postigli filtriranje paketa, postavljate skup pravila koji određuje vrste paketa (koji su sa ili za određenu IP adresu ili port) koje se prosljeđuju i koje vrste se blokiraju. (filtriranje paketa)

Perimeter network

Mreža dodana između zaštićene mreže i vanjske mreže, kako bi pružila dodatni sloj sigurnosti. Često se naziva DMZ.

Proxy server

Program koji se bavi s vanjskim poslužiteljima umjesto internih klijenata. Klijenti proxya razgovaraju s proxy poslužiteljima, koji odobrene zahtjeve klijenata prenose stvarnim poslužiteljima, a odgovore natrag klijentima.

Denial of Service

Napad kod kojeg napadač zauzima resurse na vašem računalu za stvari koje ono ne bi smjelo raditi tako sprečavajući normalno korištenje vaših mrežnih resursa za potrebne stvari.

Buffer overflow

Uobičajeni stil kodiranja nikad ne alocira "dovoljno velike" buffere i ne provjerava da li je prešao njihovu veličinu. Kada se takvi bufferi prepune, izvršni program (demon ili set-uid program) može se natjerati na neke čudne stvari. Obično to radi prepunjavanjem povratne adrese funkcije na stacku da pokazuje na drugu lokaciju.

IP spoofing

IP spoofing je složen tehnički napad koji se sastoji od nekoliko dijelova. To je sigurnosna rupa koja radi tjeranjem računala da vjeruju da ste vi netko tko zapravo niste. Opširan članak o tome objavili su daemon9, route i infinity u Phrack Magazine, 48. broj, 7. godina.

Autentication

Mogućnost saznavanja da su primljeni podaci jednaki podacima koji su poslani i da je navedeni pošiljatelj stvarni pošiljatelj. (autentifikacija)

Non-repudiation

Mogućnost primatelja da dokaže kako je pošiljatelj nekih podataka stvarno poslao te podatke, iako pošiljatelj poslije može poricati da je ikad poslao te podatke. (nezamjenjivost)

13 Često postavljana pitanja

1. Je li sigurnije kompajlirati drajver izravno u kernel umjesto kao modul?

   Odgovor: Neki misle da je bolje isključiti mogućnost učitavanja podrške za uređaje preko modula jer uljez tako može učitati trojanski modul ili sam učitati modul koji bi utjecao na sigurnost sustava.

   Međutim, da bi učitali modul, morate biti root. U datoteke modula može pisati također samo root. To znači da je uljezu potreban pristup rootu da bi ubacio modul. Ako uljez dobije pristup rootu, ima puno ozbiljnijih stvari o kojima treba brinuti nego da li će učitati modul.

   Moduli služe za dinamičko učitavanje podrške za određene uređaje koji se možda rjeđe koriste. Na strojevima koji su poslužitelji ili firewallovi na primjer, to je vrlo nevjerojatno. Iz tih razloga, za poslužitelje kompajliranje izravno u kernel ima više smisla. Također, moduli su sporiji od izravne podrške u kernelu.

2. Logiranje kao root s udaljenog stroja uvijek je neuspješno.

   Odgovor: Pročitajte dio o sigurnosti roota. To je učinjeno namjerno kako bi se udaljeni korisnici spriječili u pokušajima spajanja telnetom na vaše računalo kao root, što je ozbiljna sigurnosna rupa. Ne zaboravite, mogući uljezi vrijeme imaju na svojoj strani i mogu automatski tražiti vašu lozinku.

3. Kako da uključim shadow lozinke na svom Red Hatu 4.2 ili 5.0?

   Odgovor: Shadow lozinke su mehanizam spremanja vaših lozinki u datoteku koja nije uobičajena `/etc/passwd`. To ima nekoliko prednosti. Prva je što je shadow datoteka, `/etc/shadow`, čitljiva samo za roota, za razliku od `/etc/passwd`, koja mora ostati čitljiva za sve. Druga je prednost što vi kao administrator možete uključiti ili isključiti račune bez da svi znaju stanje računa drugih korisnika.

   Onda se datoteka `/etc/passwd` koristi za pohranjivanje imena korisnika i grupa, koje koriste programi kao što je `/bin/ls` za pretvaranje UID-a u odgovarajuće ime korisnika u sadržaju direktorija.

   Datoteka `/etc/shadow` sadrži samo korisničko ime i njegovu lozinku, te možda informacije o računu, kao što je datum njegova istjecanja, itd.

   Uključiti shadow lozinke možete naredbom `pwconv` kao root. Trebala bi se pojaviti datoteka `/etc/shadow` koju bi trebale koristiti i aplikacije. Pošto koristite RH 4.2 ili bolji, PAM moduli će se automatski prilagoditi promjeni korištenja normalne `/etc/passwd` u shadow lozinke, bez ikakvih drugih promjena.

   Pošto vas zanima osiguravanje vaših lozinki, možda će vas također zanimati generiranje dobrih lozinki na početku. Za to možete koristiti pam_cracklib modul, dio PAM-a. Vašu lozinku provjerava protiv Crack librarya kako bi vam otkrio da li ju je prelako pogoditi iz programa za razbijanje lozinki.

4. Kako da uključim Apache SSL proširenja?

   Odgovor:

   (a) Nabavite SSLeay 0.8.0 ili noviji s `<ftp://ftp.psy.uq.oz.au/pub/Crypto/SSL/>`.

   (b) Kompajlirajte, testirajte i instalirajte ga!

(c) Nabavite izvorni kod Apache 1.2.5.

(d) Nabavite Apache SSLeay proširenja s `<ftp://ftp.ox.ac.uk/pub/crypto/SSL/apache_1.2.5+ssl_1.13.tar.gz>`.

(e) Otpakirajte ga u direktoriju s izvornim kodom apache 1.2.5 i zakrpite Apache prema `README`-u.

(f) Konfigurirajte ga i kompajlirajte.

Možete pogledati i `<http://www.replay.com>`, gdje se nalaze mnogi već kompajlirani paketi, i to izvan SAD-a.

5. Kako da radim s korisničkim računima, ali zadržim sigurnost?

   Odgovor: distribucija Red Hat, posebno 5.0, sadrži velik broj alata za mijenjanje svojstava korisničkih računa.

   - Programi pwconv i unpwconv mogu se koristiti za pretvaranje u i iz shadow lozinki.
   - Programi pwck i grpck mogu se koristiti za provjeravanje pravilne organizacije `passwd` i `group` datoteka.
   - Programi useradd, usermod i userdel mogu se koristiti za dodavanje, brisanje i mijenjanje korisničkih računa. Programi groupadd, groupmod i groupdel čine isto za grupe.

   Svi ovi programi svjesni su shadowa – dakle, ako uključite shadow lozinke, koristit će `/etc/shadow` za informacije o lozinkama, ako ne, neće.

   Za daljnje informacije pogledajte odgovarajuće man stranice.

6. Kako mogu određene HTML dokumente zaštititi lozinkom koristeći Apache?

   Odgovor: Kladim se da niste znali za `<http://www.apacheweek.com/>`, ne?

   Informacije o autentifikaciji korisnika možete naći na `<http://www.apacheweek.com/features/userauth>`, kao i druge naputke za sigurnost WWW-a na `<http://www.apache.org/docs/misc/security_tips.html>`.

14 Zaključak

Ako se pretplatite na mailing liste za sigurnosne uzbune i pratite trenutne verzije, možete jako popraviti sigurnost svoga stroja. Ako pazite na svoje log datoteke i redovito pokrećete nešto poput Tripwirea, možete i više.

Na kućnom računalu nije teško održavati razumnu razinu sigurnosti. Na poslovnim strojevima potrebno je više napora, ali Linux može biti itekako sigurna platforma. Zahvaljujući prirodi njegovog razvoja, sigurnosni ispravci izlaze puno brže nego za komercijalne operacijske sustave, što Linux čini idealnim kada je sigurnost u pitanju.

15 Zahvale

Ove informacije skupljene su iz mnogih izvora. Hvala slijedećim ljudima koji su izravno ili neizravno pridonijeli:

- Rob Riggs, *rob@DevilsThumb.com*
- S. Coffin, *scoffin@netcom.com*

- Viktor Przebinda, *viktor@CRYSTAL.MATH.ou.edu*
- Roelof Osinga, *roelof@eboa.com*
- Kyle Hasselbacher, *kyle@carefree.quux.soltec.net*
- David S. Jackson, *dsj@dsj.net*
- Todd G. Ruskell, *ruskell@boulder.nist.gov*
- Rogier Wolff, *R.E.Wolff@BitWizard.nl*

16 Hrvatski prijevod

Najnovija verzija ovog prijevoda može se naći na `<http://dokumentacija.linux.hr/Sigurnost-KAKO.html>`. Održava ga Matej Vela, *mvela@public.srce.hr*. Svi su prilozi, primjedbe i prijedlozi dobrodošli.