Linux Security HOWTO

Kevin Fenzi, kevin@scrye.com & Dave Wreski, dave@nic.com
Vertaler: *Reggy Ekkebus*, *reggy@zeelandnet.nl*
v1.0.2, 25 April 1999

Dit document is een algemeen overzicht van de security onderwerpen die een administrator van een Linux systeem tegenkomt. Het houdt een algemene security gedachte in en een paar bijbehorende voorbeelden, over hoe je je Linux systeem beter kunt beveiligen tegen indringers. Er zijn ook verwijzingen naar programma's en materiaal dat met security te maken heeft. Verbeteringen, constructieve kritiek, toevoegingen en correcties zijn welkom. Mail je feedback naar bijde auteurs met "Security HOWTO" als subject.

Inhoudsopgave

1 Introductie

Dit document bevat enkele van de belangrijkste onderwerpen die te maken hebben met Linux Security. Algemene gedachten en netwerk geboren bronnen worden besproken.

Enkele andere HOWTO documenten overlappen met de security onderwerpen, en naar die document wordt verwezen waar ze ook zijn.

Dit document is *niet* bedoeld als een bij de tijds document over misbruik. Grote aantallen nieuw misbruik vindt plaats van tijd tot tijd. Dit document verteld je waar te kijken voor zulk soort informatie, en zal enkele algemene methodes geven om je er tegen te beschermen.

1.1 Nieuwe versies van dit document

Nieuwe versies van dit document zullen regelmatig naar *comp.os.linux.answers* worden gestuurd. Ze zullen worden toegevoegd aan verschillende anonieme FTP sites die zulke informatie bevatten. O.a:

ftp://metalab.unc.edu/pub/Linux/docs/HOWTO

Je zult 'm normaal gezien ook moeten vinden op de Linux World Wide Web home page via:

http://metalab.unc.edu/mdw/linux.html

De allerlaatste versie van dit document zou ook verkrijgbaar moeten zijn op:

http://scrye.com/~kevin/lsh/

1.2 Feedback

Alle opmerkingen, fout verslagen, extra informatie en kritiek van alle soorten moeten gestuurd worden naar:

kevin@scrye.com

en

dave@nic.com

Notitie: Zendt je feedback naar *beide* auteurs. Zet ook "LinuxSecurityöf "HOWTOïn je subject om Kevin's spam filter te omzeilen.

1.3 Disclaimer

Geen verantwoordelijkheid voor de inhoud van dit document kunnen worden geaccepteerd, voorbeelden en andere inhoud zijn te gebruiken op eigen risico. Toevoeging, dit is een vroege versie, er kunnen veel kleine foutjes in staan.

Een aantal voorbeelden en beschrijvingen gebruiken RedHat(tm) package indeling en systeem setup.

Zo ver we weten, alleen programma's die, onder zulke termen mogen gebruikt worden of gewaardeerd voor persoonlijke doelen worden beschreven. Veel van die programma's zijn verkrijgbaar, compleet met source, onder de *GNU* <http://www.gnu.org/copyleft/gpl.html> termen.

1.4 Copyright Informatie

Dit document is copyright (c)1998,1999 Kevin Fenzi en Dave Wreski, en is gedistributeerd onder de volgende termen:

- Linux HOWTO documenten mogen worden gereproduceerd en gedistributeerd geheel of gedeeltelijk, in elk medium, fysiek of elektronisch, zolang de copyright notitie verwerkt is in elke kopie. Commericiele re-distributie is toegestaan en aangemoedigd, hoewel, de auteurs er wel van op de hoogte gesteld moeten worden.
- Alle vertalingen, afgeleide werken, andere werken die te maken hebben met een Linux HOWTO document moet uitgebracht worden onder dit copyright. Dat is, je mag een HOWTO document niet

reproduceren en enkele beperkingen toevoegen. Uitzonderingen op deze regels mogen worden gegeven onder bepaalde omstandigheden; Neem contact op met de HOWTO coördinator op het onderstaande adres.

- Als je vragen hebt, neem dan contact op met Tim Bynum, de Linux HOWTO coordinator,

tjbynum@metalab.unc.edu

2 Overzicht

Dit document zal enkele procedures en vaak gebruikte software om je Linux systeem veiliger te proberen uit te leggen. Het belangrijkste is dat we eerst de basis concepten bespreken, zodat we een soort security basis krijgen, voordat we beginnen.

2.1 Waarom hebben we Security nodig

In de altijd veranderende wereld van globale data communicatie, goedkope Internet connecties, en snelle software ontwikkeling is security een steeds belangrijker onderwerp. Security is nu een basis behoefte, omdat internet zeer onveilig is. Als je data van punt A naar B gaat over het internet, kan het door verschillende andere punten gaan onderweg, dat geeft andere gebruikers de mogelijkheid het te onderscheppen en ze kunnen het zelfs veranderen. Zelfs gebruikers om jouw systeem kunnen je data veranderen in iets anders wat je niet bedoelde. Onbevoegde toegang tot je systeem kun verschaft worden door indringers, ook wel bekend als "crackers", die dan gevorderde wetenschap gebruiken om je privacy te schenden, je informatie stelen of je zelfs je toegang tot je eigen files te ontzeggen. Als je benieuwd bent naar de verschillen tussen een "Hackerën een "Cracker", kijk dan in Eric Raymond's document, "How to become A Hacker", verkrijgbaar op: *http://sagan.earthspace.net/˜esr/faqs/hacker-howto.html*.

2.2 Hoe veilig is veilig?

Eerst, houdt in gedachten dat geen computer systeem ooit helemaal veilig kan zijn. Je kunt het alleen heel moeilijk maken voor iemand om je systeem binnen te dringen. Voor de gemiddelde Linux thuis gebruiker, is niet veel nodig om de cracker buiten de deur te houden. Voor high tech linux gebruikers (banken, telecommunicatie bedrijven, etc), is veel meer werk vereist.

Een andere factor om te onthouden is hoe beter je systeem beveiligd is, hoe minder je met je systeem kunt doen. Je moet beslissen waar de balans te vinden voor jouw systeem zodat het bruikbaar blijft, en ook nog veilig is voor jouw gedachten. Bijvoorbeeld, je zou iedereen kunnen laten in-bellen en ze dan thuis terug bellen. Dit is veiliger, maar als iemand niet thuis is, wordt het moeilijk voor hem om inteloggen. Je zou ook je linux systeem kunnen instellen zonder netwerk en zonder internet, maar dat is niet nodig.

Als je een groot tot gemiddeld bedrijf hebt, moet je een security politiek maken beginnend met hoeveel security je in je bedrijf nodig hebt. En wie/wat dat gaat controleren. Een voorbeeld van een bekende security politiek is *http://ds.internic.net/rfc/rfc2196.txt*. Het is pas aangepast, en het bevat een groot lijstwerk voor het maken van een security politiek voor jouw bedrijf.

2.3 Wat probeer je te beschermen?

Voordat je je systeem probeert veilig te maken, moet je eerst vast stellen waartegen je je moet beschermen, welke risico's je moet nemen en welke niet, en hoe gevoelig je systeem is als gevolg hiervan? Je moet je systeem analyseren om te weten wat je beschermt, waarom je het beschermt, welke waarde het heeft, en wie de verantwoordelijk heeft voor je data en ander bezit.

- Risico is de mogelijkheid dat een indringer succesvol binnenkomen in je computer. Kan een indringer files lezen of schrijven of programma's draaien die schade kunnen veroorzaken? Kan hij belangrijke data weggooien? Kan hij jouw of je bedrijf van belangrijk werk ontdoen? Niet vergeten: iemand toegang geven to je account, of je computer, kan ook je privacy bloot leggen. En, als je een in-secure account hebt op je systeem kan het hele netwerk worden binnen gedrongen. Als je een gebruiker laat inloggen door de `.rhosts` file, of een andere onveiligere manier, zoals `tftp`, loop je het risico dat een indringer binnen komt. Als een indringer een account heeft op je systeem, of op het systeem van iemand anders, kan hij dat gebruiken om toegang te krijgen tot een ander account of een ander systeem.

- Een gevaar is iemand die motivatie heeft om een netwerk of een computer binnen te dringen. Je moet beslissen wie je moet vertrouwen om op je systeem te komen, en welk gevaar dat kan veroorzaken. Er zijn verschillende types van indringers, en het is makkelijk om hun verschillen te onthouden als je je systeem beveiligd.

  - **De nieuwsgierige** - Dit type indringer is normaal geïnteresseerd in welk systeem en data je hebt.
  - **De kwaadwillige** - Dit type van indringers is er op uit om je computer uit te zetten of je web pagina te bekladden of anders dwingt hij je om geld en tijd te spenderen om zijn schade te herstellen.
  - **De geavanceerde indringer** - Dit type indringer probeert je systeem te gebruiken om populair en gevreesd te worden. Hij kan je systeem gebruiken om te adverteren over de dingen die hij kan.
  - **De mededinger** - Dit type indringer is geïnteresseerd in welke data je hebt op je systeem. Het kan iemand zijn die denkt dat je iets hebt waarvan hij kan profiteren, finanancieel of iets anders
  - **De lener** - Dit type indringer is geïnteresseerd in het opzetten van een winkel op je systeem en de bronnen gebruiken voor eigen doel. Ze zullen een chat of irc server draaien, een porno site, of zelfs een DNS server.
  - **De gebruiker** - Dit type indringer is alleen geintersseerd in je systeem om het te gebruiken om in andere systemen te komen. Als je systeem veel connecties heeft of een gateway is naar verschillende interne computers, dan kun je dit type vaak zien om je systeem in te nemen.

- Gevoeligheid beschrijft hoe goed je systeem beschermt is van ander netwerk, en de mogelijkheid voor iemand om ongewilde toegang te krijgen.

  Wat is er aan de hand als iemand je systeem binnendringt? Natuurlijk de bezorgdheid van een dynamisch PPP thuis gebruiker zijn anders dan die van een groot bedrijf dat zijn computers aan het internet hangt, of een ander groot netwerk.

  Hoeveel tijd neemt het in om de data die verdwenen was op te halen of opnieuw te maken? Een tijdige tijd investering kan later tien maal zoveel tijd besparen als je je data opnieuw moet aanmaken als het verdwenen is. Heb je je backup strategie onderzocht, en laatst je data nagekeken?

2.4 Een security politiek ontwikkelen

Maak een simpele, algemene politiek voor je systeem dat gebruikers kunnen begrijpen en opvolgen. Het zou je data die je waarborgt moeten beschermen en ook de privacy van de gebruikers. Enkele andere dingen die je zou moeten overwegen zijn: Wie hebben toegang tot het systeem (Kan mijn vriend mijn account gebruiken?), wie mag software op het systeem installeren, wie is de eigenaar van data, rampen verbetering, en wie mag het systeem gebruiken.

Een algemene goede security politiek start met de volgende zin

Dat wat niet toegestaan is, is verboden

Dat betekend dat tenzij je toegang geeft tot een bepaalde dienst aan een gebruiker. Weet zeker dat die politiek wel werkt op je reguliere gebruikers account. Zeggen, "Ah, ik kan dat permissie probleem niet oplossen, ik doe het wel even als root"kan tot security gaten leiden en die zijn erg opvallend, en zelfs de genen die nog niet misbruikt zijn.

rfc1244 is een document dat beschrijft hoe je een netwerk veiligheids politiek moet maken.

rfc1281 is een document dat een voorbeeld laat zien van een veiligheids politiek met gedetailleerde beschrijvingen van elke stap.

Tot slot, je kan ook kijken naar het COAST politiek archief op *ftp://coast.cs.purdue.edu/pub/doc/policy* om te zien hoe een echte veiligheids politiek er uit ziet.

2.5 Bedoelingen van het beveiligen van je netwerk

Dit document zal verschillende middelen bespreken om de dingen waar je hard voor hebt gewerkt te beschermen: je lokale machine, je data, je gebruikers, je netwerk, en zelfs je reputatie. Wat gebeurt er met je reputatie als een indringer de data van een gebruiker weggooit? Of je web pagina beklad? Of de kolectieve plannen publiceert van je bedrijf voor het volgende kwartaal? Als je een netwerk installatie plant, zijn er vele factoren waar je rekening mee moet houden voordat je een enkele computer aan het netwerk toevoegt.

Zelfs als je een enkel in-bel PPP account hebt, of maar een klein bedrijf, wil dit niet betekenen dat indringers niet geïnteresseerd zijn in je systeem. Grote high-tech bedrijven zijn niet het enige doel. Veel indringers willen simpelweg zoveel mogelijk netwerken binnendringen, voor hen maakt het niet uit welk netwerk het is. En, ze kunnen een beveiligings gat in je netwerk gebruiken om op een ander netwerk te komen waarmee jij in verbinding staat.

Indringers hebben heel veel geduld, en kunnen mijden hoe je je systeem hebt verduisterd, door gewoon alles te proberen. Er zijn een hele hoop dingen waarom een indringer geïnteresseerd kan zijn in je systeem, maar dat bespreken we later.

2.5.1 Host Security

Het gebied van security waar systeem administrator het meest op gericht zijn is host security. Dit betekend meestal je eigen systeem veilig maken en hopen dat iedereen op het netwerk hetzelfde doet. Goede paswoorden kiezen, de lokale netwerk diensten van je host veilig maken, alles goed bijhouden en programma's upgraden met een security gat. Dat is wat een systeem administrator moet doen. Hoewel dit zeer nodig is, wordt dit een vervelend werkje als je een netwerk hebt met meer dan een paar computers.

2.5.2 Netwerk Security

Netwerk security is even belangrijk als host security. Met honderd, duizend, of zelfs meer computers op het zelfde netwerk, kun je niet vertrouwen op elk systeem apart. Beloven dat alleen goedgekeurde gebruiker het netwerk kunnen gebruiken, bouw firewalls, gebruik sterke versleuteling, en weet zeker dat er geen onveilige machines zijn op het netwerk. Dit zijn ook allemaal Systeem Administrator taken.

Dit document zal enkele van de technieken bespreken die gebruikt worden om een netwerk te beveiligen, en we hopen je te laten zien hoe je een indringer buiten de deur houdt om er zo voor te zorgen dat hij niet aan de data kan komen die jij probeert te beschermen.

2.5.3 Security door onbekendheid

Een type van security dat moet besproken worden is "Security door onbekendheid"Dat betekend bijvoorbeeld, dat je een dienst verplaats die bekend is als een zwakke schakel naar een andere niet standaard poort in de hoop dat aanvallers het niet opmerken en het dus niet misbruiken. Security door onbekendheid is geen security. Simpel, omdat als je een klein netwerk hebt, of niet echt een high-tech netwerk kan een indringer toch nog interesse hebben.

2.6 Organisatie van dit Document

Dit document is verdeeld in een aantal secties. Deze verslaan enkele globale security onderwerpen. De eerste, 3 (Fysieke Security), houdt in hoe je fysieke security moet verzorgen. De tweede, 4 (Lokale Security), beschrijft hoe je je systeem moet beschermen tegen aanvallen van lokale gebruikers. De derde 5 (Files en Filesystem Security), laat zien hoe je je filesysteem moet instellen en permissies zetten op je files. De volgende, 6 (Passwoord Security en Encryptie), bespreekt hoe je encryptie moet gebruiken om je machine en je netwerk beter te beveiligen. 7 (Kernel Security) bespreekt welke kernel opties je moet nemen om een veiliger systeem te creeëren. 8 (Netwerk Security), beschrijft hoe je je Linux systeem beter kunt beveiligen tegen netwerk aanvallen. 9 (Security voorbereidingen), bespreekt hoe je je machine er op moet voorbereiden om hem online te brengen. Daarna, 10 (Wat te doen onder en na een inbraak), bespreekt wat je moet doen als een er inbraak plaatsvindt of hoe een te detecteren die pas is gebeurt. In 11 (Security Bronnen), worden enkele primaire security bronnen opgesomd. De V en A sectie 13 (Veel gestelde vragen), beantwoordt enkele veel gestelde vragen, en tot slot een conclusie in de 14 (Conclusie) sectie.

De twee algemene punten om te realiseren als je dit document leest zijn:

- Houdt je systeem in de gaten. Kijk in de systeem log files zoals `/var/log/messages` en houdt een oog op je systeem. En,
- Houdt je systeem up to date door altijd de nieuwste versies van software te installeren en upgrade op security alarm. Dit doen maakt je systeem al veel veiliger.

3 Fysieke Security

De eerste laag van security is de fysieke security van je systeem. Wie heeft er directe fysieke toegang tot je computer? Moeten ze dat? Kan je je machine beschermen tegen hun aanvallen? Moet je dat?

Hoeveel fysieke security je nodig hebt op je systeem hangt af van je situatie, en/of budget.

Als je thuis gebruiker bent, hebt je niet zoveel nodig (hoewel je kan je machine moeten beschermen tegen je kinderen die het kapot proberen te maken of een vervelend familielid). Als je in een Lab bent, heb je veel meer fysieke security nodig, maar de gebruikers moeten nog steeds hun werk kunnen doen op de machine. Veel van de volgende secties zullen je uit de problemen helpen. Als je op een kantoor bent, moet je je computer wel of niet beveiligen in je vrije uren of als je weg bent. Bij sommige bedrijven, als je je computer daar laat staan, onbeveiligd is dat een overtreding.

Eenvoudige fysieke security methodes zoals sloten op deuren, kabels, gesloten kastjes, en video bewaking zijn ook goede ideeën, maar dat is buiten beschouwing van dit document:)

3.1 Computer sloten

Veel moderne PC kasten hebben ook een öp slot"mogelijkheid. Normaal is dit een kontakt aan de voorkant van de computer kast dat je instaat stelt om de computer in gesloten of open positie te zetten. Kast sloten kan helpen tegen diefstal van je computer, of de kast openen en direct de hardware stelen. Dit kan ook soms ook helpen tegen iemand die je computer wil opstarten met z'n eigen hardware of floppy.

Deze kast sloten doen andere dingen dan de steun in het moederbord en hoe de kast gemaakt is. Op veel PC maken ze het zo dat je de kast eerst moet open breken om erin te komen. Op sommige andere maken ze het zo dat je geen ander toetsenbord kan in pluggen of een andere muis. Kijk in het boekje van je moederbord of de kast instructies voor meer informatie. Dit kan soms een zeer nuttige eigenschap zijn, omdat de sloten vaak van zeer lage kwaliteit zijn kunnen aanvallers ze vaak makkelijk openbreken.

Sommige kasten (meestal Sparc's en Mac's) hebben een hardware-sleutel aan de achterkant waar je een kabel door kan doen, aanvallers moeten dan de kabel doorknippen of de kast breken om er in te komen. Een hangslot of een combinatie slot erdoor en het wordt al een stuk moeilijker voor iemand om je computer te stelen.

3.2 BIOS Security

De BIOS is het laagste niveau van software dat een x86 hardware configureert en in werking stelt. Lilo en andere Linux start methodes kijken in de BIOS om te kijken hoe ze je Linux machine moeten starten. Andere hardware waar Linux op draait heeft dergelijke software (OpenFirmware op Macs en nieuwe Suns, Sun boot PROM, etc...). Je kan je BIOS gebruiken om een aanvaller tegen te houden om je linux systeem opnieuw op te starten en te gebruiken.

Veel PC Bios-en laten je een boot pas-woord instellen. Dit houdt niet veel Security in(de BIOS kan ge-reset worden, of verwijderd als iemand in de kast kan komen), maar het kan goed afschrikken (o.a het kost tijd en laat sporen achter). Op de zelfde manier, op S/Linux (Linux voor een SPARC(tm) processor), kun je de EEPROM ook instellen om om een boot pass-woord te vragen. Dat vertraagt aanvallers.

Veel x86 BOISen laten je ook andere goede security settings instellen. Kijk in je BIOS manual of kijk er naar de volgende keer als je re-boot. Bijvoorbeeld, enkele Bios-en laten je niet van floppy booten en sommige vragen een pas-woord om enkele BIOS dingen in te stellen.

Notitie: Als je een server hebt, en je zet er een boot pas-woord op dan kun je de machine niet zonder aandacht laten opstarten. Onthoudt dat je moet komen om het pas-woord in te tikken als de stroom is uitgevallen. ;(

3.3 Boot Loader Security

De verschillende Linux boot loaders kunnen ook een boot pas-woord hebben. LILO, bijvoorbeeld, heeft een `password` en `restricted` instelling. `password` vraagt altijd om een pass-woord en `restricted` vraagt om een password als je een optie achter linux zet (zoals `single`), bij de `LILO:` prompt natuurlijk.

Onthoudt dat als je als deze pas-woorden instelt je ze ook nog moet onthouden. :) Onthoud ook dat deze pas-woorden de aanvaller vertragen. Dit houdt ze niet tegen om je computer te booten van flop en dan je root partitie te mounten. Als je security gebruikt in samenwerking met de boot Loader, kun je booten van een floppy ook uitzetten in de BIOS van je computer en de BIOS met een pas-woord beschermen.

Als iemand security gerelateerde informatie heeft over de verschillende boot loaders, zouden we dat graag willen horen. (`grub`, `silo`, `milo`, `linload`, etc).

Notitie: Als je een server hebt, en je zet er een boot pas-woord op dan kun je de machine niet zonder aandacht laten opstarten. Onthoudt dat je moet komen om het pas-woord in komen tikken als de stroom is uitgevallen. ;(

3.4 Xlock en V lock

Als je van tijd tot tijd weg gaat bij je machine is het leuk als je je scherm kunt "locken", zodat niemand met je werk kan knoeien of je werk kan zien. Daar zijn twee programma's voor: `xlock` en `vlock`.

`xlock` is een X display locker. Het zou bij elke linux distributie moeten zitten die X support. Kijk in de man page voor meer informatie over de opties, maar normaal kun je het starten met `xlock` vanuit elke xterm op je console en het zal de display locken en een pas-woord vragen om het te unlocken.

`vlock` is een simpel klein programma dat je instaat stelt om enkele of alle virtuele consoles op je Linux box te locken. Je kunt enkel de gene waar je in werkt locken of allemaal. Als je er maar een doet kunnen andere achter je computer komen en je console gebruiken; ze kunnen het virtuele console dat je gelockt hebt niet gebruiken totdat je het weer hebt ge-unlockt. `vlock` zit bij RedHat Linux.

Natuurlijk, je console locken zal iemand tegen houden om je werk te verknoeien, maar het houdt hem niet tegen je machine te re-booten of je werk verstoren. Het houdt hen ook niet tegen om je computer via het netwerk te bereiken om zo problemen te veroorzaken.

Belangrijker, het houdt iemand niet tegen van X weg te switchen en naar de gewone console te gaan, of naar het VC waarvan jij X hebt gestart. Zo kunnen ze je X stoppen en hebben ze jouw privileges. Je zou beter Xdm kunnen draaien, bijvoorbeeld.

3.5 Een Fisieke Security aanval detecteren

Het eerste waar je naar moet kijken is of je machine is gereboot. Linux is een robuust en stabiel OS, de enige keer dat je re-boot is als jij je computer plat legt voor een OS upgrade, hardware verwisseling, of zoiets. Als je machine opnieuw is opgestart zonder dat jij het deed, kan dat een signaal zijn van 'er is een indringer geweest'. Veel van de manieren hoe je computer aangevallen kan worden, willen eerst dat de computer is ge-reboot of uitgezet.

Kijk voor signalen van knoeien op de kast en in het computer gebied. Hoewel veel indringers sporen van hun aanwezigheid uit de log files halen, is het een goed idee om in de log files te kijken voor enige tegenstellingen

Het is ook een goed idee om je log data op een veilige plek te bewaren, zoals een aparte log server in je goed beschermde netwerk. Als je machine is aangevallen is log data belangrijk, ook als het is aangepast door de indringer.

De syslog deamon kan zo worden geconfigureerd dat deze de log files naar een centrale syslog server zend, maar dit wordt normaal gezonden als clear text. Dus de indringer kan de data zien als het wordt getransporteerd. Dit kan informatie dat niet publiek is onthullen over je netwerk. Er zijn syslog deamons verkrijgbaar die de data encrypted zenden.

Onthoud ook dat het heel simpel is om syslog messages te vervalsen - met een misbruik programma dat is gemaakt. Zal syslog zelfs messages accepteren van het netwerk met als host local host, zonder dat syslog naar de werkelijke afkomst kijkt.

Enkele dingen om in je logs te checken:

- Korte of incompele logs.
- Logs met een vreemde tijd.
- Logfiles met verkeerde permissies.
- Regeltjes van re-boot en het stop/starten van een dienst.
- missende stukjes log.

- su invoer en login van een vreemde plaats.

We zullen log data 9.4 (later) in de HOWTO nog bespreken.

4 Lokale Security

Het volgende wat we gaan doen is je systeem beschermen tegen lokale gebruikers. Zijn er *lokale* gebruikers? Ja!

Toegang krijgen tot het account een lokale gebruiker is het eerste wat een indringer doet om toegang te krijgen tot het root account. Met lakse lokale security, kunnen ze hun normale account ü̈pgraden"naar het root account door gebruik van een aantal bugs en armzalig opgezette lokale diensten. Als je zorgt dat je lokale security goed is, heeft de indringer nog een hindernis die hij voorbij moet komen.

Lokale gebruikers kunnen een hoop schade aanrichten op je systeem (speciaal) als ze zijn hoe ze zeggen dat ze zijn. Een account verstrekken aan mensen die je niet kent of geen informatie over hebt is een slecht idee.

4.1 Een nieuw account aanmaken

Je moet een gebruikers account maken met de minimale benodigd heden voor de taken die hij moeten doen. Als je een account wilt maken voor je zoon (10 jaar), kun je hem alleen toegang geven tot een text verwerker of een tekenprogramma, maar hem niet de mogelijkheid geven om data te deleten dat niet van hem is.

Enkele goede aanwijzingen om iemand een veilig account te geven op je Linux machine:

- Geeft ze de minimale rechten die ze nodig hebben.
- Kijk wanneer/waar ze moeten inloggen, of wanneer ze niet moeten inloggen.
- Verwijder inactieve accounts
- Het gebruik van het zelfde user-ID op elke computer en netwerk is aanteraden om het account onderhoud makkelijk te maken, en het makkelijker maken van het analyseren van log data.
- De creatie van groep, user-IDs moet absoluut verboden zijn. Gebruikers accounts hebben ook accountability, en dat is niet mogelijk met een groep account.

Veel gebruikers account's die gebruikt worden bij een aanval zijn die die maanden of jaren niet gebruikt zijn. Omdat niemand ze gebruikt, is het een ideaal aan-vals 'voertuig'

4.2 Root Security

Het meest gevaarlijke account op je machine is dat van root (super-user). Dit account heeft bevoegdheid over de gehele machine, en dat kan ook betekenen bevoegdheid over andere machines op het netwerk. Onthoud dat je het root account alleen moet gebruiken voor hele kort, specifieke taken, en je moet meestal draaien als een normale gebruiker. Zelfs kleine foutjes als je in-gelogd bent als root kunnen problemen veroorzaken. Hoe korter je root ben hoe veiliger je bent.

Enkele trucks om te voorkomen dat je je computer overhoop haalt als root:

- Als je complexe commando's moet uitvoeren doe ze dan eerst op de niet-vernietigende manier.. vooral commando's die wildcards gebruiken: b.v, als je `"rm foo*.bar"`

  wilt doen, doe dan eerst `"ls foo*.bar"` en kijk dan of je de files weg gooit die je wilde weggooien. `echo` gebruiken i.p.v vernietigende commando's werkt soms ook.

- Voorzie je gebruikers van een standaard alias voor het rm commando om te vragen voor bevestiging voordat je ze files weggooien.
- Wordt alleen root om enkele specifieke taken uit te voeren. Als je probeert uit te vinden hoe iets werkt ga dan eerst terug naar de gewone gebruiker, totdat je `zeker` weet wat je moet doen als root.
- Het commando path voor de root gebruiker is erg belangrijk. Het commando path (dat is het `PATH` variabel) specificeert de directories waar de shell moet kijken voor programma's. Probeer het commando path voor de root gebruiker zoveel mogelijk te beperken, en zet er nooit `.` (dat betekend "de actuele directorie") in. En, zorg dat je nooit schrijf-bare directories in je PATH hebt, dit kunnen aanvallers de mogelijkheid geven nieuwe binaries in je path te zetten, dat kan betekenen dat ze de volgende keer root zijn als je dat commando draait.
- Gebruik nooit het rlogin/rsh/rexec stel van tooltjes (genoemd de r-utilities) als root. Ze zijn onderwerp van elk soort aanval, en ze zijn absoluut gevaarlijk om te draaien als root.
- Maak nooit een `.rhosts` file voor root.
- In de `/etc/securetty` file staat een lijst van terminals waar root van mag inloggen. Standaard (bij Red Hat Linux) zijn dit alleen de virtuele consoles(vtys). Wees voorzichtig met het toevoegen van iets anders aan die file. Je moet kunnen inloggen als je eigen reguliere gebruiker vanaf een andere computer en dan `su` draaien als je moet (hopelijk over `6.4 (ssh)` of een ander versleuteld kanaal), dus het is niet nodig om direct als root in teloggen.
- Altijd langzaam en oplettend als root draaien. Je acties kunnen een hoop dingen betreffen. Denk voor je typt!

Als je iemand absoluut root toegang moet geven (hopelijk iemand die je goed vertrouwd) op je machine zijn daar enkele hulp middelen voor. `sudo` geeft gebruikers de mogelijkheid om hun eigen pas-woord te gebruiken om een aantal commando's te mogen gebruiken als root. Dit geeft je de mogelijkheid, bijvoorbeeld, om een gebruiker de mogelijkheid te geven om removable media(cdrom, etc...) te mounten en eruit halen op je linux machine, maar ze hebben geen andere root rechten. `sudo` houdt ook een log file bij van alle succesvolle en on-succesvolle sudo pogingen, dit geeft je de mogelijkheid om te kijken wie welk commando gebruikte voor wat. Daarom werkt `sudo` goed in plaatsen waar een paar mensen root moeten zijn, omdat het je instaat stelt om te zien wat ze doen.

Hoewel `sudo` specifieke gebruikers specifieke rechten kan geven voor specifieke taken, heeft het toch tekort komingen. Het zou alleen maar moeten worden gebruikt voor taken als de server re-starten, een gebruiker toevoegen. Elk programma dat een shell escape heeft geeft root toegang tot de gene die het programma heeft gestart heeft. Dit zijn bijvoorbeeld de meeste editors. Ook een onschadelijk programma as `/bin/cat` kan gebruikt worden om files teoverschrijven, dit kan veroorzaken dat het root account wordt misbruikt. beschouw `sudo` als een verantwoording, maar verwacht niet dat het het root account kan vervangen en dan nog steeds secure is.

5 Files en Filesystem Security

Een paar minuten van voorbereiding en planning voordat je je systemen online zet kan helpen om ze te beschermen en de data erop ook.

- Er moet nooit een reden zijn om vanuit de homedir van users een SUID/SGID commando te draaien. Gebruik de `nosuid` optie in `/etc/fstab` voor partities die schrijf-baar zijn voor gebruikers die niet root zijn. Je kan ook `nodev` en `noexec` gebruiken op de user's home partitie, en ook `/var`, dit verbied het draaien van programma's en het aanmaken van character en block devices, wat eigenlijk nooit nodig is.
- Als je een filesysteem exporteert met NFS, configureer je `/etc/exports` dan met de meest beperkende toegang mogelijk. Dit betekend geen wildcards, geen root schrijf toegang, en zoveel mogelijk als read-only(alleen lezen) exporteren.
- Configureer je users file creatie `umask` zo beperkt mogelijk. Zie ook 5.1 (umask settings).
- Als je een filesysteem gebruikt over het netwerk met NFS, configureer dan je /etc/fstab met goede beperkingen. Zoals, 'nodev'. 'nosuid', en misschien 'noexec'.
- Zet filesysteem limitaties ipv alles toestaan, zoals het default is. Je kan dat per gebruiker instellen door gebruik te maken van de resource-limits PAM module en `/etc/pam.d/limits.conf`. Bijvoorbeeld, limieten voor de groep `users` kan er zo uitzien:

```
@users     hard  nproc   50
@users     hard  rss     5000
```

  Dit zegt dat het verboden is om core files te maken, dat er maar 50 processen magen draaien, en maar 5M geheugen.
- De `/var/log/wtml` en `/var/run/utml` files bevatten de login lijst van alle gebruikers op je systeem. Hun eenheid moet bewaard blijven, want het kan gebruikt worden om vast te stellen wanneer en van waar een gebruiker (of een mogelijke indringer) het systeem is binnen gekomen. Deze files moeten ook de `644` permissie hebben, zonder het beïnvloeden van het normale systeem.
- De immutable bit kan gebruikt worden om per ongeluk deleten of overschrijven van een file tegen te gaan een file die beschermt moet worden. Het houd ook iemand tegen om een symbolic link naar de file te maken (zulke symbolische links zijn een bron van aanvallen die verwijder van `/etc/passwd` en `/etc/shadow` to gevolg hebben). Zie de `chattr`(1) man page voor meer informatie over het immutable bit.
- SUID en SGID files op je systeem zijn een mogelijk security risico, en moet nauwlettend in de gaten gehouden worden. Omdat deze programma's extra rechten geven aan de persoon die ze gebruikt, het is nodig dat in-secure programma's niet worden geïnstalleerd. Een favoriete truck van crackers is een SUID-root programma misbruiken, en dan een SUID programma achter laten als een achterdeur om de volgende keer door die achterdeur binnen te komen, zelfs als het originele gat is dichtgestopt. Vindt alle SUIT/SGID programma's op je systeem en houdt deze in de gaten, dus wees bewust van elke verandering, die kan duiden op een waarschijnlijk indringer. Gebruik het volgende commando om alle SUID/SGID programma's op je systeem te vinden:

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

  De Debian distributie draait een job elke nacht om vast te stellen welke SUID files er zijn. Het vergelijkt ze dan met de vorige nacht. Je kan kijken in `/var/log/suid*` voor een log.

  Je kan het SUID of SQID permissie verwijderen op een verdacht programma met `chmod`, dan het terug veranderen als je het nodig vindt.

- Wereld schrijf-bare files, vooral systeem files, kunnen een security hole zijn als een cracker toegang to je systeem weet te verkrijgen en ze dan veranderd. Wereld schrijf-bare directories zijn gevaarlijk, doordat ze een cracker files laten toevoegen en verwijderen als hij dat wil. Om alle wereld schrijf-bare files op te sporen, gebruik dan het volgende commando:

```
root# find / -perm -2 ! -type l -ls
```

  En weet zeker waarom deze files schrijf-baar zijn. In de normale gang van zaken , zijn enkele files wereld leesbaar, inclusief enkele van `/dev`, en symbolische links, dus de `! -type l` haalt ze uit het vorige `find` commando.

- Files zonder eigenaar kunnen ook ook een indicatie van een indringer zijn. Je kan alle files zonder eigenaar en groep op je systeem vinden door het volgende commando:

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

- Alle `.rhosts` files vinden zou een van je reguliere taken moeten zijn als systeem administrator, omdat deze files niet zijn toegestaan op je systeem. Onthoud een cracker heeft maar een in-secure account nodig om toegang te krijgen tot het hele netwerk. Je kunt alle `.rhosts` files op je systeem vinden door het volgende commando:

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

- Tot slot, voordat je de permissies veranderen op iedere systeem file, weet dan zeker wat je doet. Verander nooit permissies op een files omdat dat je makkelijkste weg lijkt om iets werkende te krijgen. Altijd eerst vaststellen waarom de file die permissies heeft voordat je het veranderd.

5.1 Umask Instellingen

Het `umask` commando kan gebruikt worden om de standaard file creatie mode op je systeem in te stellen. Het is de octale aanvulling op de verzochte file mode. Als een files is aangemaakt zonder om te kijken naar hun permissie instellingen, kan de gebruiker lees en schrijf bevoegdheden geven aan iemand die dat niet mag. Meestal bevatten de `umask` instellingen `022`, `027` en `077` (wie het meest beperkt is). Normaal is het umask ingesteld in `/etc/profile`, zodat het betrekking heeft op elke gebruiker op het systeem. Het file aanmaak mask kan uitgerekend worden door de gewilde permissies van 777 af te trekken. In andere woorden, een umask van 777 zou betekenen dat de file niet leesbaar, niet schrijf-baar of niet uitvoerbaar is voor iedereen. Een mask van 666 zou betekenden dat de file een mask heeft van 111. Bij voorbeeld, je kan een regel hebben als deze:

```
# Set the user's default umask
umask 033
```

Weet zeker dat je root's umask `077` maakt, dat schakeld lezen, schrijven en uitvoer rechten voor iedere ander gebruiker uit, tenzij deze is veranderd met `chmod`. Be sure to make root's umask `077`, which will disable read, write, and execute permission for other users, unless explicitly changed using `chmod`. In dit geval zou een nieuwe directore de 744 permissies hebben, verkregen door 033 van 777 aftetrekken. Nieuwe files met het 033 mask hebben de 644 permissie.

Als je Red Hat gebruik, en de gebruiker zit alleen in een groep met een zelfde naam (User Private Groups), is `002` voldoen als `umask`. Dit is doordat de standaard configuratie is 1 gebruiker per groep.

5.2 File Permissies

Het is belangrijk dat je systeem files niet open zijn voor het zomaar bewerken van gebruikers en groepen die niet zulk systeem onderhoud moeten doen.

Unix verdeeld toegang controle op files en directories over drie groepen: owner(eigenaar), group(groep) en other(andere). Er is altijd een eigenaar, elk aantal leden van een groep, en de rest.

Een snelle uitleg over Unix rechten(permissions): A quick explanation of Unix permissions:

Eigendom(ownership) - Welke gebruiker(s) en groep(en) heeft(hebben) controle over de permissies over de node en de moeder node.

Permissies - Bits capable of being set or reset to allow certain types of access to it. Permissies van directories kunnen verschillende betekenissen hebben dan die van files.

Lezen:

- De mogelijkheid om de file te lezen
- De mogelijkheid om in de directorie te kijken.

Write:

- De mogelijkheid om een file te veranderen, toe te voegen of verwijderen.
- De mogelijkheid om files in een directorie te verplaatsen, verwijderen of toevoegen.

Uitvoeren:

- De mogelijkheid om binary programma's of shell scripts uit te voeren
- De mogelijkheid om te zoeken in de directory in combinatie met het lees recht

Text attributen opslaan: (voor directories)

Het "sticky bit"heeft ook een andere betekenis op directories dan op files. Als de sticky bit op een directory staat mag iemand alleen files weg gooien als hij de eigenaar is, zelfs als hij schrijf rechten heeft op de directorie. Alleen als er uitzonderlijke rechten worden toegewezen mag hij de file weggooien. Dit is gemaakt voor directories als `/tmp`, die voor iedereen schrijf-baar zijn, maar waar het niet gewild is dat iedereen zomaar elke file kan weggooien. De sticky bit is te zien als een `t` in een lange directorie lijst.

SUID Attribuut: (Voor files)

Dit beschrijft het set-user-id recht op een file. Als de set user ID toegangs mode is ingesteld in de eigenaars rechten, en de file is uitvoerbaar, processen die het draaien hebben toegang de systeem bronnen als de eigenaar van de file, in tegenstelling to de gene die het proces startte. Dit is de oorzaak van veel "buffer overflow"misbruik.

SGID Attribuut: (Voor file)

Als dit ingesteld is in de groep permissies, houdt dit bit het "set group id"status van een file. Dit gedraagt zich net als SUID, alleen de groep is beïnvloed. De file moet uitvoerbaar zijn voor dit.

SGID Attributen: (Voor directories)

Als je het SGID bit op een directorie instelt (met `chmod g+s` *`directorie`*), files die aangemaakt worden in die dir hebben als groep de groep die eigenaar is van de directorie.

Jij - De eigenaar van de file

Groep - De groep waar de file aan toebehoord

Iedereen - Iedereen op het systeem die niet de eigenaar is of in de groep hoort.

File Voorbeeld:

```
-rw-r--r--  1 kevin  users        114 Aug 28  1997 .zlogin
1st bit - directorie?                (nee)
 2nd bit - lezen door eigenaar?       (ja, door kevin)
  3rd bit - schrijven door eigenaar?    (ja, door kevin)
   4th bit - uitvoeren door eigenaar?    (nee)
    5th bit - lezen door groep?           (ja, door users)
     6th bit - schrijven door groep?       (nee)
      7th bit - uitvoeren door groep?       (nee)
       8th bit - lezen door iedereen?        (ja, door iedereen)
        9th bit - schrijven door iedereen?    (nee)
         10th bit - uitvoeren door iedereen?   (nee)
```

De volgende regels zijn voorbeelden van de minimale instellingen van rechten om aan de er achter getypte rechten te voldoen. Je kan meer rechten willen geven dan hieronder staan beschreven, maar dit moet beschrijven wat deze minimale rechten met files doen:

```
-r--------  Lees rechten op de file voor de eigenaar
--w-------  Laat de eigenaar de file aanpassen of weggooien
            (Notitie dat iedereen met schrijf rechten op de directory
             de file kan overschrijven en dus verwijderen)
---x------  De eigenaar kan het programma uitvoeren, maar geen shell script
            want deze hebben ook lees rechten nodig.
---s------  Laar de file uitvoeren met een effectief User ID = aan eigenaar
--------s-  Laat de file uitvoeren met een effectief Group ID = aan de groep
-rw------T  Geen update van "laatst veranderd tijd". Meestal voor swap files.
---t------  Geen effect. (sticky bit)
```

Directory Voorbeeld:

```
drwxr-xr-x  3 kevin  users        512 Sep 19 13:47 .public_html/
1st bit - directorie?                 (ja, er staan veel files in)
 2nd bit - lezen door eigenaar?       (ja, door kevin)
  3rd bit - schrijven door eigenaar?    (ja, door kevin)
   4th bit - uitvoeren door eigenaar?    (ja, door kevin)
    5th bit - lezen door groep?           (ja, door users)
     6th bit - schrijven door groep?       (nee)
      7th bit - uitvoeren door groep?       (ja, door users)
       8th bit - lezen door iedereen?        (ja, door iedereen)
        9th bit - schrijven door iedereen?    (nee)
         10th bit - uitvoeren door iedereen?   (ja, door iedereen)
```

De volgende regels zijn voorbeelden van de minimale instellingen van rechten om aan de er achter getypte rechten te voldoen. Je kan meer rechten willen geven dan hieronder staan beschreven, maar dit moet beschrijven wat deze minimale rechten met directories doen:

```
dr--------  De inhoud kan bekeken worden, maar de file attributen kunnen niet gelezen worden
d--x------  Je kan de directory binnen gaan, en je kan hem gebruiken in een lang uitvoer path
dr-x------  De file attributen kunnen gelezen worden door eigenaar.
d-wx------  Files kunnen worden aangemaakt en verwijderd, zelfs als het niet de actieve directorie is
d------x-t  Hou het tegen voor anderen met schrijf rechten om files weg te gooien. Gebruikt in /tmp
d---s--s--  Geen effect.
```

Systeem configuratie files (Normaal in `/etc`) hebben meestal de `640` mode (`-rw-r---`) en root is de eigenaar. Afhankelijk van je bedrijfs security eisen, kun je dit veranderen. Laat een systeem file nooit schrijf-baar door een groep of iedereen. Enkele configuratie files, zoals `/etc/shadow`, moeten alleen leesbaar zijn voor root, en directories in `/etc` moeten op z'n minst niet toegankelijk zijn voor anderen.

SUID Shell Scripts

SUID shell scripts zijn een serieus security risico, en daardoor laat de kernel die scripts niet toe. Ongeacht van hoe secure je denkt dat je shell script is, het kan worden misbruikt om een cracker een root shell te geven.

5.3 Integriteit verificatie met `Tripwire`

Een ander zeer goede manier voor het detecteren van locale aanvallen (en ook op het netwerk) op je systeem is het draaien van een intergeriteit controleur zoals `Tripwire`. `Tripwire` draait een aantal controles op alle belangrijke binaries en configuratie files en vergelijkt ze met een database met de vorige files, goed voor een opmerking. Dus, elke verandering in een file wordt aangegeven.

Het is een goed idee om `Tripwire` te installeren op een floppy, en dan het floppy fysiek op write protected zetten. Door dit kunnen indringers niet met `Tripwire` zelf knoeien en ook de database niet veranderen. Zodra `Tripwire` hebt geïnstalleerd, is het een goed idee om het te draaien als een van je normale security administratie taken om te zien of er iets is veranderd.

Je kan het ook toevoegen aan je `crontab` en `Tripwire` elke nacht van je floppy laten draaien en je resulten 's morgens laten mailen. Zoiets als:

```
# set mailto
MAILTO=kevin
# run Tripwire
15 05 * * * root /usr/local/adm/tcheck/tripwire
```

zal je elke morgen om 5:15 een verslag sturen.

`Tripwire` kan een geluk zijn om indringers te detecteren voor dat je ze zelf opmerkt. Doordat een hoop files veranderen op het gemiddelde systeem, moet je onderscheid maken tussen wat je jouw werk is en wat het werk van een cracker is.

Je kunt `Tripwire` vinden op *http://www.tripwiresecurity.com*, Gratis. Handboeken en steun kan gekocht worden.

5.4 Trojaanse paarden

"Trojaanse paarden"zijn genoemd naar de fabelachtige strategie in Homer's "Iliad". Het idee is dat een cracker een programma maakt of een binary dat geweldig lijkt, en andere mensen aanmoedigt het te downloaden en het te draaien als root. Dan kan het programma hun systeem kraken als ze geen aandacht besteden.

Terwijl ze denken dat het programmaatje dat ze net uitgevoerd hebben maar een ding doet, heeft het wel hun security doorbroken.

Je moet oppassen met de programma's die je installeert op je machine. Redhat heeft MD5 controles en PGP handtekeningen op hun RPM files zodat je kan verificeren dat het is wat je denk. Andere distributies hebben soortgelijke methoden. Je moet niet zomaar ieder onbekend programma draaien, vanwaar je geen source hebt, als root! Veel aanvallers willen een source code uitgeven aan het publieke onderzoek.

Hoewel het complex is, haal altijd je source van een echt distributie site. Als het gaat draaien als root, kijk dan eerst naar de source en bevestig deze.

6 Password Security en Versleuteling

Een van de meest belangrijke security onderwerpen van vandaag de dag zijn pas-woorden. Het is belangrijk dat jij en de andere gebruikers een secure en onraad-baar pas-woord hebben. De meest recente Linux distributies hebben het `passwd` programma dat je niet instaat stelt om een makkelijk raad-baar pas-woord te nemen. Weet zeker dat je `passwd` programma deze opties heeft en bij de tijd is.

Een diepgaande discussie over Versleuteling is te ver gaand voor dit document, maar een kleine introductie is wel op z'n plaats. Versleuteling is erg handig, misschien is het zelfs nodig. Er zijn allemaal verschillende methoden van data encryptie, allemaal met z'n eigen eigenschappen.

De meeste Unicies (een Linux is geen uitzondering) gebruiken standaard een manier van ecriptie, genoemd DES (Data encryptie standaard) op je pas-woorden te ver-sleutelen De ver-sleutelde pas-woorden staan (normaal) in `/etc/passwd` (of minder vaak in) `/etc/shadow`. Als we proberen in te loggen, wordt het pas-woord dat we ingetypt hebben weer versleuteld en vergeleken met het pas-woord in de pas-woord file. Als ze gelijk zijn, mag je inloggen, want de pas-woorden moeten wel hetzelfde zijn. Hoewel DES een twee weg versleutelings algoritme is (je kan de en-coderen en decoderen, als je de goede sleutel geeft), de variant die most unices is een een weg versleutelings algoritme. Dit betekend dat het niet mogelijk is om te achterhalen wat er staat in `/etc/passwd` (of `/etc/shadow`) heeft gestaan.

Brute sterke aanvallen, zoals "Crack of "John the Ripper"(zie sectie 6.9 ()) kunnen vaak het pas-woord raden tenzij je pas-woord voldoende toevallig is. De PAM module (zie hieronder) geeft je de mogelijkheid om een andere versleutelings routine te nemen (MD5 of iets anders). Je kan Crack ook gebruiken voor eigen voordeel. Probeer Crack te runnen op je pas-woord database om in-secure pas-woorden te vinden. Dan neem je contact op met de desbetreffende gebruiker, en vraag je hem zijn pas-woord te veranderen.

Je kan gaan naar*http://consult.cern.ch/writeup/security/security_3.html* om informatie te vinden over hoe je een goed pas-woord moet kiezen.

6.1 PGP en Public-Key Versleuteling

Public-Key versleuteling, zoals PGP die gebruikt, gebruikt een sleutel voor encryptie en een voor decrytie. Traditionele versleuteling, gebruikt meestal maar een sleutel voor encryptie en een voor descriptie; deze sleutel moet bij beide partijen bekend zijn, en dus moet het verstuurd worden van de een naar de ander, veilig.

Om de behoefte van het veilig sturen van een versleutelings sleutel te verzachten, gebruikt Public-Key versleuteling twee verschillende sleutels: een publieke sleutel en een prive sleutel. Ieders prive sleutel is verkrijgbaar voor iedereen om de encryptie te doen, maar de prive sleutel van iedereen moet bewaard blijven. Om messages te de-crypten met hun prive sleutel met het versleuteld zijn met de correcte publieke sleutel.

Er zijn voordelen aan beiden public key en prive key versleuteling, en je kan de verschillen tussen die twee lezen in *de RSA Versleutelings FAQ* `<http://www.rsa.com/rsalabs/newfaq/>`, PGP (Pretty Good Privacy) is goed ondersteund in Linux. Versie 2.6.2 en 5.0 werken goed. Voor een goede inleiding op PGP en hoe het te gebruiken kijk in de PGP FAQ: *http://www.pgp.com/service/export/faq/55faq.cgi*

Weet zeker dat je de goede versie voor je land gebruik. Door export beperkingen van de regering van de VS, sterke versleuteling is verboden om ge transporteert te worden in elektronische data van buiten de VS.

VS export controle wordt nu gedaan door EAR (Export Administration Regulations). Dat gebeurt niet meer door ITAR.

Er is ook een stap voor stap gids voor het configureren van PGP in linux, deze is te vinden op: *http://mercury.chem.pitt.edu/~angel/LinuxFocus/English/November1997/article7.html*. Het is geschreven voor de Internationale versie van PGP, maar het is makkelijk te gebruiken voor de VS versie. Misschien heb je ook wel een patch nodig voor de nieuwste versies voor Linux; de patch is verkrijgbaar op *ftp://metalab.unc.edu/pub/Linux/apps/crypto*.

Er is een project voor een gratis her uitvoering van pgp met open source. GnuPG is een compleet en gratis vervanger voor PGP. Omdat IDEA of RSA niet gebruikt kan het worden worden gebruikt zonder beperkingen. GnuPG is bijna compatible met RPC2440 (OpenPGP). Kijk op de GNU Privacy Guard web pagina voor meer info: *http://www.gpg.org/*.

Meer informatie over versleuteling kan gevonden worden in de RSA versleutelings FAQ, verkrijgbaar op *http://www.rsa.com/rsalabs/newfaq/*. Hier vindt je info over termen als "Diffie-Hellman", "Public-Key cryptography", "digitaal certificaten", etc.

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

Vaak vragen gebruikers de verschillen tussen de verschillende security en versleutelings protocollen, en ze ze moeten gebruiken. Often users ask about the differences between the various security and encryption protocols, and how to use them. Terwijl dit geen security document is, is het toch een goed idee om globaal uitte-leggen wat elk protocol is, en waar je meer informatie kan vinden.

- **SSL:** - SSL, of Secure Sockets Layer, is een versleutelings methode gemaakt door Netscape om security over het internet aan tebieden. Het ondersteund enkele verschillende versleutelings methoden, en verzorgt ook client en server authenticatie. SSL handelt op de transport laag, het maakt een secure versleuteld kanaal van data, en kan dus naadloos data ver-sleutelen van verschillende soorten. Dit is vaak te zien als je naar een secure web-site gaat en een secure online document bekijkt met Communicator en dient als basis voor secure communicaties met Communicator, net als andere Netscape Communicaties dat versleuteling. Meer informatie kan gevonden worden op *http://www.consensus.com/security/ssl-talk-faq.html*. Informatie over Netscape 's andere security uitvoeringen is een goed startpunt voor deze protocollen verkrijgbaar op *http://home.netscape.com/info/security-doc.html*.
- **S-HTTP:** is een ander protocol dat voorziet in beveiligingsservices over het Internet. Het werd ontworpen om te voorzien in vertrouwelijkheid, authenticatie, integriteit, en zonder verwerping-en (kan niet per abuis voor iemand anders aangezien worden). Het biedt ondersteuning voor meerdere vormen van sleutel-beheer mechanismen en crypto-grafische algoritmen via option negotiation tussen de betrokken partijen in iedere transactie. S-HTTP is beperkt tot de specifieke software dat het implementeert, en versleutelt ieder bericht individueel. (Afkomstig uit de RSA Cryptography FAQ, pagina 138).
- **S/MIME:** - S/MIME, of Secure Multipurpose Internet Mail Extension, is een versleuteld standaard om electronishe post te ver-sleutelen en andere typen berichten op het internet. Het is een open standaard ontworpen door RSA, dus het is mogelijk dat we het binnenkort in Linux zien. Meer informatie over S/MIMI kan gevonden worden op *http://home.netscape.com/assist/security/smime/overview.html*.

6.3 Linux IPSEC Uitvoering

Samen met CIPE, en andere vormen van data versleuteling, zijn er ook nog een aantal andere uitvoeringen van IPSEC voor Linux. IPSEC is een operatie van de IETF om een versleutelings-secure communicaties te maken op een IP netwerk, en om verificatie te verzorgen, intergeriteit, toegang controle en vertrouwen. Informatie over IPSEC en Internet ontwerp kan gevonden worden op *http://www.ietf.org/html.charters/ipsec-charter.html*. Je kan er ook links vinden naar andere protocollen die betrekking hebben op sleutel controle en een IPSEC mailing lijst met archieven

De x-kernel Linux uitvoering, die wordt ontwikkeld op de Universiteit van Arizona, gebruikt een object gebaseerd lijstwerk voor het uitvoeren van het netwerk protocol genoemd x-kernel, het kan gevonden worden op *http://www.cs.arizona.edu/xkernel/hpcc-blue/linux.html*. Simpel weg, de x-kernel is een methode van passerende berichten op kernel niveau, dat maakt de uitvoering makkelijker.

Een andere gratis verkrijgbare IPSEC uitvoering is Linux FreeS/WAN IPSEC. Hun home page verklaard,

> "Deze diensten stellen je in staat om veilige tunnels te bouwen door on-vertrouwde netwerken. Alles dat door het on-vertrouwde netwerk gaat wordt versleuteld door de IPSEC gateway machine en weer gedecrypt aan de andere kant van de tunnel. Het resultaat is een Virtual Private Network of VPN. Dit een netwerk dat effectie prive zelfs als het machine betreft op verschillen de plaatsen op de wereld verbonden door het onveilige Internet.

Het is te downloaden op *http://www.xs4all.nl/˜freeswan/*, en is aan versie 1.0 als we dit document schrijven.

Als met andere vormen van versleuteling is het niet uitgegeven met de kernel standaard door de export beperkingen.

6.4 `ssh` (Secure Shell) en `stelnet`

`ssh` en `stelnet` zijn programma's die je instaat stellen om inteloggen op een andere computer met een ver-sleutelde verbinding.

`ssh` is een pakket van programma's gebruikt als een veilige vervanger voor `rlogin`, `rsh` en `rcp`. Het gebruikt Public-Key versleuteling om de communicaties tussen twee computers te ver-sleutelen, net als de gebruikers te verifiëren. Het kan gebruikt worden om veilig in te loggen op een andere computer of om data tussen twee computers te zenden, terwijl het man-in-the-middle attacks en Dns spoofing tegen gaat. Het gebruikt data compressie op je connecties, en secure X11 communicaties tussen de hosts. De `ssh` home kan gevonden worden op *http://www.cs.hut.fi/ssh/*

Je kan `ssh` ook gebruiken om van je Windows machine naar je linux machine `ssh` server te gaan. Er zijn verschillende gratis Windows ssh clienten zoals de client op: *http://guardian.htu.tuwien.ac.at/therapy/ssh/* ook de commercieële uitvoering van DataFellows, op *http://www.datafellows.com*. Er is ook een open source project opnieuw uit te rusten genoemd "pssst..."Voor meer informatie zie: *http://www.net.lut.ac.uk/psst/*

SSLeay is een gratis uitvoering van Netscape's Secure Sockets Layer protocol, ontwikkeld door Eric Young. Het bevat enkele applicaties, zoals Secure telnet, een module voor Apache, verschillende database, zo wel als verschillende algorithme's zoals DES, IDEA en Blowfish.

Als je deze bibliotheek gebruik, is er een secure telnet vervanger die de telnet connectie versleuteld. Het met SSH is dat stelnet SSL gebruikt, het Secure Socket Layer protocol ontwikkeld door Netscape. Je kan Secure telnet en Secure FTP vinden door de starten met de SSLeay FAQ, verkrijgbaar op *http://www.psy.uq.oz.au/˜ftp/Crypto/*.

SRP is een andere secure telnet/ftp uitvoering. Van hun web pagina:

> "Het SRP project ontwikkeld secure Internet software, gratis voor wereldwijd gebruik. Startend met een geheel secure Telnet en FTP distributie, we hopen zwakke netwerk verificatie te vervangen met sterke vervangers die niet verliezen met gebruikers vriendelijke security. Security moet de standaard zijn, niet een optie!"

Voor meer informatie, ga naar *http://srp.stanford.edu/srp*.

6.5 PAM - Pluggable Authentication Modules

Nieuwere versies van de Red Hat Linux distributie leveren een samengebonden bevestigings schema genoemd "PAM". PAM stelt je in staat om je bevestigingen en benodigdheden gelijk te veranderen, en alle lokale bevestigings methoden veranderen zonder dat je het opnieuw moet compileren. PAM configureren hoort niet tot dit document, maar ga eens kijken op de PAM web-site voor meer informatie. *http://www.kernel.org/pub/linux/libs/pam/index.html*.

Een paar dingen die je kan doen met PAM:

- Een andere encryptie methode dan DES gebruiken voor je pas-woorden. (Het moeilijker maken om ze zomaar de decoden)
- Bronnen limieten instellen voor al je gebruikers zodat ze je diensten niet kunnen tegenwerken (aantal processen, hoeveelheid geheugen, etc)
- Shadow passwords aanzetten (zie hieronder).
- Gebruikers alleen laten inloggen op bepaalde tijden en van bepaalde plaatsen.

In een paar uur van installeren en con-figuren van je systeem, kan je veel aanvallers tegenhouden voordat ze verscheinen. Bijvoorbeeld, kun je PAM gebruiken om `.rhosts` uit te zetten, door een regel aan `/etc/pam.d/rlogin` toetevoegen:

```
#
# Disable rsh/rlogin/rexec for users
#
login auth required pam_rhosts_auth.so no_rhosts
```

6.6 Cryptographic IP Encapsulation (CIPE)

Het belangrijkste doel van deze software is een middel aan te bieden voor veilige(tegen afluisteren, met o.a verkeer analyse, en vervalste berichten injectie) sub-netwerk interconnecite over een onveilig packet netwerk als Internet.

CIPE versleuteld de data op de netwerk laag. Packet-en die tussen de computers reizen worden versleuteld. De encryptie motor is geplaatst naar de driver die de packet-ten ontvangt en verstuurd.

Dit is niet net als SSH, wie de data versleuteld bij de connectie, op de socket laag. Een logische connectie tussen twee programma's die draaien op verschillende computers word versleuteld.

CIPE kan gebruikt worden voor tunneling, om bijvoorbeeld een Virtual Private Netwerk te maken. Het lage encryptie niveau heeft voordelen dat het transparant werkt tussen twee computers die zitten in het VPN, zonder verandering in de applicatie software.

> Overgenomen uit de CIPE documentatie: De IPSEC standaard defineerd een aantal protocollen die gebruikt kunnen worden (met andere dingen) om ver-sleutelde VPN's te maken.

> Hoewel, IPSEC een zwaar en complex protocol is met een hoop opties, uitvoeringen van de full protocol versie zijn nog maar zelden gebruikt en sommige delen (zoals een sleutel manager) zijn nog steeds niet helemaal klaar. CIPE gebruikt een soortgelijke aanpak, waarin veel dingen als parameter ingesteld worden(zoals de gebruikte versleutelings methode die gebruikt wordt) zijn een installatie optie. Dit limiteert de flexibiliteit, maar het is dan wel een simpelere (en daardoor efficient, makkelijk te debuggen...) uitvoering.

Meer informatie kan gevonden worden op *http://www.inka.de/˜bigred/devel/cipe.html*

Net als andere vormen van versleuteling, is het niet gedistributeerd met de kernel door de export limitaties.

6.7 Kerberos

Kerberos is een verificatie systeem ontwikkeld door het Athena Project op MIT. Als een gebruiker inlogt, Kerberos bevestigd de gebruiker (doormiddel van een paswoord) en geeft hem de mogelijkheid zijn identiteit door te-geven aan andere servers en computers verspreid over het netwerk.

Deze bevestiging is dan gebruikt door andere programma's zoals `rlogin` om gebruikers de mogelijkheid te geven om op andere computers inteloggen zonder pas-woord (ipv de `.rhosts` file).

Kerberos en andere programma's die erbij zitten, houden gebruikers tegen om het systeem te "bedriegen"zodat ze denken dat je iemand anders bent. Helaas, is het installeren van Kerberos een zeer opdringerig, vragend om verandering en vervanging van een aantal standaard programma's

Je kan meer informatie vinden over Kerberos op *the Kerberos FAQ*, en de code is te vinden op *http://nii.isi.edu/info/kerberos/.*

[Van: Stein, Jennifer G., Clifford Neuman, and Jeffrey L. Schiller. "Kerberos: Een bevestigings dienst voor een Open netwerk systeem."USENIX Conference Proceedings, Dallas, Texas, Winter 1998.]

Kerberos moet niet je eerste stap zijn om veiligheid te bevorderen op je hosts. Het is best ingewikkeld, en het is niet veel gebruikt, zeg, SSH.

6.8 Shadow Passwords.

Shadow passwords wordt gebruikt om je versleutelde pas-woorden geheim te houden voor normale gebruikers. Anomaal zijn deze versleutelde pas-woorden opgeslagen in de `/etc/passwd` file voor iedereen te lezen. Iedereen kan er dan een programmaatje op loslaten om te kijken welke het zijn. Shadow passwords, worden opgeslagen in `/etc/shadow`, deze file kan alleen gelezen worden door de mensen die dat mogen. Om shadow passwords te gebruiken, moet je al je programmaatjes her compileren die de /etc/passwd file gebruiken. PAM (hierboven) geeft je ook de mogelijkheid om de shadow module er zo in te zetten; het is niet nodig dat de uitvoerbare bestanden worden ge her compileert. Je kan in de Shadow-Password HOWTO kijken voor meer informatie als deze nodig is. Hij is verkrijgbaar op *http://metalab.unc.edu/LDP/HOWTO/Shadow-Password-HOWTO.html* Het is goed bij de tijd, en hoeft geen distributie met PAM.

6.9 "Crackën "John the Ripper"

Als om een of andere reden je `passwd` programma niet dwingt om moeilijk te raden pas-woorden te nemen, kun je een pas-woord kraak programmaatje draaien om zeker te weten dat je gebruikers moeilijk te raden pas-woorden nemen.

Pas-woord kraak programma's werken op een simpel idee: ze proberen elk woord in het woordenboek, en dan variaties op die woorden, vesleutelen ze en kijken of deze gelijk is aan je versleutelde pas-woord. Als ze een zelfde vinden weten ze je pas-woord.

Er zijn een aantal van die programmatjes... de twee meest bekende zijn "Crackën "John the Ripper"(*http://www.false.com/security/john/index.html*) . Ze nemen wel een hoop van je cpu tijd in, maar het loont de moeite, want als je de pas-woorden eruit haalt die slecht zijn, heeft de aanvaller niets meer aan het programma. Onthoudt dat een aanvaller altijd eerst een paar andere gaten probeert om de `/etc/passwd` te lezen, maar zulke gaten zijn meer gewoon dan je zou denken.

Omdat security alleen sterk is als er geen zwakke hosts zijn, is het de moeite als je Windows machine(s) op je netwerk checkt met L0phtCrack, een Crack uitvoering voor Windows. Het is verkrijgbaar op *http://www.l0pht.com*

6.10 CFS - Cryptographic File System en TCFS - Transparent Cryptographic File System

CFS is een manier om een gehele directorie structuur te versleutelen en de gebruikers in staat stellen om er versleutelde files in te zetten. Het gebruikt een NFS server op de locale machine. De RPM is verkrijbaar op *http://www.replay.com/redhat/*, en meer informatie over hoe het werkt op *ftp://ftp.research.att.com/dist/mab/*.

TCFS verbeterd CFS door meer integratie te bieden met het file systeem, zodat het transparant is voor de gebruiker dat het filesysteem versleuteld is. meer informatie op: *http://edu-gw.dia.unisa.it/tcfs/*.

Het is niet nodig om het op het gehele filesysteem te gebruiken. Het werkt ook op alleen directories.

6.11 X11, SVGA en display security

6.11.1 X11

Het is belangrijk om je grafische display te beschermen tegen indringers die je pas-woorden overnemen terwijl je het typt, informatie lezen op je scherm, of zelfs een gat gebruiken om root toegang te krijgen. Remote X applicaties draaien over een netwerk kan ook een gevaar zijn, sniffers kunnen al je contacten met de andere computer zien.

X heeft een aantal toegangs controle mechanismen. De simpelste van deze is computer-gebaseerd: je gebruikt `xhost` om in te stellen welke machines toegang hebben tot je X display. Dit is helemaal niet secure, want als iemand toegang heeft tot je machine, kunnen ze `xhost` *`+hun machine`* doen en ze kunnen gemakkelijk binnen komen. Ook, als je ook ondertrouwde machines toegang moet geven tot je display kan iedereen je display overnemen.

Als je `xdm` (X Display Manager) gebruikt om in te loggen, krijg je een veel betere toegangs methode: MIT-MAGIC-COOKIE-1. Een 128-bit "cookie"wordt gegenereerd en opgeslagen in `.Xauthority`. Als je een andere machine toegang moet geven tot je display kun je het `xauth` commando gebruiken en de info in je `.Xauthority` file gebruiken om alleen die connectie toe te staan. Zie de Remote-X-Apps mini-howto, verkrijgbaar op *http://www.nl.linux.org/doc/HOWTO/Remote-X-Apps-NL.html*.

Je kan `ssh` ook gebruiken (zie 6.4 (), hierboven) om secure X connecties toe te staan. Dit heeft als voordeel dat alle data wordt versleuteld en dat er niets naar het netwerk weg lekt.

Kijk in de `Xsecurity` man pagina voor meer informatie over X security. Het veiligste om te gebruiken is `xdm` om in te loggen op je console en dan `ssh` te gebruiken om naar andere computers te gaan en daar je X programma's draaien.

6.11.2 SVGA

SVGAlib programma's zijn typisch SUID-root om toegang te krijgen to je Linux machines video hardware. Dit maakt ze er gevaarlijk. Als ze crashen, moet je re-booten om een bruikbaar console terug te krijgen. Weet zeker dat de SVGA programma's die je draait vertrouwbaar zijn, zo dat ze nog een beetje te vertrouwen zijn. Nog beter, draai ze helemaal niet.

6.11.3 GGI (Generic Graphics Interface project)

Het Linux GGI project probeert problemen op te lossen met het video interface in linux. GGI verplaatst een klein deel van de video code in de kernel, en dan neemt het controle over het video systeem. Dit betekend dat GGI instaat is om je console te herstellen en het zo weer goed te maken. Ze hebben ook een security waarschuwings sleutel, zodat je zeker weet dat er geen Trojan horse `login` programma's draaien. *http://synergy.caltech.edu/~ggi/*

7 Kernel Security

Dit is een beschrijving van de kernel configuratie opties die te maken hebben met security, en een uitleg wat ze doen en hoe ze te gebruiken.

Als de kernel je netwerk op je computer beheerst, is het belangrijk dat het erg veilig is, en dat het niet misbruikt kan worden. Om enkele van laatste netwerk aanvallen tegen te gaan, moet je je kernel versie goed houden. Je vind nieuwe kernels op `<ftp://ftp.kernel.org>` of van je distributie leverancier.

7.1 2.0 Kernel Compilatie Opties

Voor 2.0.x kernels, hebben de volgende opties effect. Je moet de opties zijn onder het kernel configuratie proces. Veel van het commentaar is uit `./linux/Documentation/ Configure.help`, Dat is dezelfde help als in het `make config` proces van de kernel.

- Network Firewalls (CONFIG_FIREWALL) Deze optie zou aan moeten staan als je een firewall of masquerading wilt draaien op je linux machine. Als het gewoon een algemene client machine wordt, is het veilig om nee te zeggen.
- IP: forwarding/gatewaying (CONFIG_IP_FORWARD) Als je IP forwarding aanzet, wordt je Linux machine een router. Als je machine op het netwerk is, kun je data van het ene naar het andere netwerk doorsturen, en misschien een firewall zetten om dat te voorkomen. Normale dail-up gebruikers zullen dit uitzetten, en andere zullen zicht concentreren op de security overwegeningen om dit te doen. Firewall willen dit aan hebben staan, en is gebruikt in combinatie met de firewall software.

  Je kan IP forwarding dynamisch aanzetten met het volgende commando:

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

  en weer uit met:

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

  Onthoud deze files, en hun grote, weerkaats niet hun eigenlijke grootte, en ondanks worden ze leeg, mag of mag niet.

- IP: syn cookies (CONFIG_SYN_COOKIES) Een "SYN Aanvalïs een denial of service (DoS) aanval die alle systeem bronnen 'opeet' op je machine, zodat je moet re-booten. We kunnen geen reden bedenken waarom je dit moet uitzetten. In de 2.1 kernel series staat deze optie !!mearly!! syn cookies toe, maar zet ze niet aan. Om ze aan te zetten doe:

  ```
  root# echo 1 > /proc/sys/net/ipv4/tcp_syncookies <P>
  ```

  Deze optie is nodig als je je machine gaat configureren als een firewall, of als je masquerading gaat doen, of als je je dail-up computer wilt beschermen tegen iemand die wil binnen dringen via je PPP dail-up interface.

- IP: firewall packet logging (CONFIG_IP_FIREWALL_VERBOSE) Deze optie geeft je informatie over packets die je firewall ontvangt, zoals zender, ontvanger, poort, etc.

- IP: Drop source routed frames (CONFIG_IP_NOSR) Deze optie moet aan staan. Source gerouteerde frames houden het gehele pad naar hun bestemming in het pakket. Dit betekend dat routers waar het pakket door gaat niet het pakket eerst moeten inspecteren maar het gelijk kunnen doorsturen. Dit kan leiden tot data die je systeem binnen gaat en een mogelijke aanval kan zijn.

- IP: masquerading (CONFIG_IP_MASQUERADE) Als er een van de computers op je lokale netwerk waar je Linux doos als firewall voor dient iets naar buiten wilt zenden, kan je linux machine de host "masqueraden", b.v, stuurt het het verkeer door naar de bedoelde bestemming, maar het laat het eruit zien of het van de firewall doos kwam. Zie *http://www.indyramp.com/masq* voor meer informatie.

- IP: ICMP masquerading (CONFIG_IP_MASQUERADE_ICMP) De optie voegt ICMP masquerading to toe aan de vorige optie van het alleen masqueraden van TCP of UDP verkeer.

- IP: transparent proxy support (CONFIG_IP_TRANSPARENT_PROXY) Dit stelt je Linux firewall in staat om transparant elk netwerk verkeer van het lokale netwerk en bestemd van een andere computer naar een lokale server genoemd een "transparante proxy server"door te sturen. Dit laat de lokale computers denken dat ze met de andere computer aan het 'praten' zijn, maar ze praten met de lokale proxy-server. Zie de IP-Masquerading HOWTO en *http://www.indyramp.com/masq* voor meer informatie

- IP: always de-fragment (CONFIG_IP_ALWAYS_DEFRAG) Normaal is deze optie uitgeschakeld, maar als je een firewall bouwt of een masquerading host, moet je dit aanzetten. Als data wordt gezonden van de ene host naar de andere, wordt het niet altijd gezonden als een packet van data, maar meestal is het opgesplitst in enkele delen. Het probleem hiermee is dat het poort-nummer alleen is opgeslagen is het eerste deel van het pakketje. Dat betekend dat iemand informatie in die andere pakketjes kan steken wat er niet hoort. Het kan ook een teardrop aanval tegen een interne host tegen houden die er niet tegen is beschermd.

- Packet Signatures (CONFIG_NCPFS_PACKET_SIGNING) Dit is een optie die verkrijgbaar is in de 2.1 kernel series die NCP paketjes signeert voor sterkere security. Normaal kun je het uitzetten, maar het is er als je het nodig hebt.

- IP: Firewall packet netlink device (CONFIG_IP_FIREWALL_NETLINK) Dit is een erg handige optie die je instaat stelt op de eerste 128 bytes van een packet te analyseren in een user-space programma, om vast te stellen of je het packet wilt accepteren of wilt tegenspreken, gebaseerd op zijn geldigheid.

7.2 2.2 Kernel Compilatie Opties

Voor 2.2.x kernels zijn veel van de opties hetzelfde, maar enkele nieuwe zijn ontwikkeld. Veel van de beschrijvingen komen uit `./linux/Documentation/Configure.help` welke dezelfde help is als dir onder het `make` `config` proces van het compileren van de kernel. Alleen de nieuwe opties zijn beschreven hieronder. De meest opvallende verandering in de 2.2 kernel is de Ip firewalling code. Het `ipchains` programma wordt nu gebruikt om de IP firewall code te installeren, ipv het `ipfwadm` programma gebruikt in de 2.0 kernel.

- Socket Filtering (CONFIG_FILTER) Voor de meeste mensen, is het veilig om hier nee te zeggen. Deze optie geeft je de mogelijkheid om een user-space filter aan elke socket vast te maken en dan vaststellen of een pack wordt binnengelaten of niet. Tenzij je een het echt nodig hebt en zulke filters kunt programmeren, je moet nee zeggen. Notitie: het ondersteund alle protocol-en behalve TCP.
- Port Forwarding Port Forwarding is een toevoeging op IP Masquerading die je instaat stelt om pakketten door te sturen van buiten de firewall naar binnen een firewall op gegeven poorten. Dit kan makkelijk zijn als bijvoorbeeld je wilt een web-server draaien achter een firewall of ip masquerading host en de web-server moet toegankelijk zijn voor de buitenwereld. Een externe client zend een vraag naar poort 80 van de firewall, de firewall stuurt deze vraag door naar de web-server, de web-server neemt deze vraag aan en stuurt de informatie naar de externe client. De client denkt dat de firewall machine zelf een web-server draait. Dit kan ook gebruikt worden voor gebruik balancering als je een aantal identieke web servers hebt achter een firewall.

  Informatie over dit onderwerp is verkrijgbaar van http://www.monmouth.demon.co.uk/ipsubs/portforwarding.html (om het WWW te browsen, moet je toegang hebben to een machine op het Internet dat een programma heeft als netscape of lynx). Voor algemene informatie, zie ftp://ftp.compsoc.net/users/steve/ipportfw/linux21/
- Socket Filtering (CONFIG_FILTER) Als je deze optie gebruikt, kan een user-space programma een filter vastmaken aan elke socket en daardoor vertellen dat de kernel een pakket moet toestaan of niet toestaan van een bepaalt type data om door de socket te komen. Linux socket filtering werkt op alle socket types behalve TCP voor nu. Zie de text file `./linux/Documentation/networking/filter.txt` voor meer informatie.
- IP: Masquerading De 2.2 kernel masquerading is verbeterd. Het heeft nu ook support voor speciale protocollen om te masqueraden, etc. Leest de IP Chains HOWTO voor meer informatie.

7.3 Kernel Devices

Er zijn een aantal block en character devices onder Linux die je helpen met je security.

De twee devices `/dev/random` en `/dev/urandom` zijn beschikbaar gesteld door de kernel en kunnen je toevallige data geven op elk moment.

Beiden `/dev/random` en `/dev/urandom` moet allebij secure genoeg zijn in het gebruik om PGP keys te maken, `ssh` uitdagingen, en andere applicaties waar secure toevallige nummers nodig zijn. Aan vallers moeten het volgende nummer niet kunnen voorspellen en zo achterhalen welk nummer jij had. Er is veel moeite in gestopt om zeker te weten dat je altijd in een toevallig nummer krijgt zoals het woord zegt.

Het enige verschil is dat `/dev/random` stop met het geven van toevallig bytes en wacht tot ze zich ophopen. Notitie: Op sommige systemen kan het een lange tijd stil staan wachtend op een nieuwe gebruiker-genereerde invoer die moet worden ingevoerd in de computer. Dus je moet nadenken voordat je `/dev/random` gebruikt. (Misschien is het beste om het te gebruiken wanneer je een gevoelige sleutel genereert, en de gebruiker op het keyboard laat typen totdat je print "Ok, genoeg".)

`/dev/random` is hoge kwaliteit entropie, gegenereerd door het meten van inter-interrupt tijden etc. Het blokkeert totdat er genoeg bits toevallige dat is.

`/dev/urandom` is het hetzelfde, maar wanneer de uitrusting van entropie laag begint te worden, zal het een versleutelde sterke hash geven van wat er is. Dit is niet secure, maar het is genoeg voor de meeste applicaties.

Je kan lezen van de devices door het gebruik als dit:

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

Dit print zes toevallig karakters op het console, goed voor pas-woord generatie. Je vind `mmencode` in het `metamail` package.

Zie `/usr/src/linux/drivers/char/random.c` voor een beschrijving van het algoritme.

Dank aan Theodore Y. Ts'o, Jon Lewis, en andere van de Linux-kernel voor het helpen van mij (Dave) met dit.

8 Netwerk Security

Netwerk security is steeds meer en meer belangrijk als mensen meer en meer tijd verbonden zijn. Netwerk security doorbreken is meestal veel gemakkelijker dan fysiek of lokaal aanvallen, en is normaler.

Er zijn een aantal goede tools om je te helpen met netwerk security en meer en meer van deze zitten bij de Linux distributies.

8.1 Pakket Sniffers

Een van de toegankelijke manieren waarmee indringer toegang krijgen tot meer systemen op je netwerk is door het gebruik van een packet sniffer op een al eerder binnen gedrongen computer. Deze "sniffer"luistert op de Ether-net poort voor dingen als `passwd`, `login` en `su` in de packet stroom en logt het verkeer daarna. Op deze manier, krijgen aanvallers pas-woorden van systemen waar ze niet eens van plan waren om op in te breken. Clear-text pas-woorden zijn erg kwetsbaar voor deze aanvallen.

Voorbeeld: Host A is gekraakt. Aanvaller installeren een sniffer. Sniffer onderschept een admin die inlogt op Host B vanaf Host C. Het pakt de admin's persoonlijke pas-woord als hij inlogt op B. Dan doet de admin een `su` om een probleem op te lossen. Nu hebben ze het root pas-woord van Host B. Later laat de admin iemand `telnetten` vanaf zijn account naar Host Z op een ander netwerk. Nu heeft de aanvaller een pas-woord/login op Host Z.

In deze dagen en jaren, hoeft een aanvaller niet eens een systeem meer aan te vallen om dit te doen: ze kunnen ook een laptop of pc in het gebouw brengen en deze aan het netwerk pluggen en zo sniffen.

Door het gebruik van `ssh` of andere encrypted pas-woord methoden worden deze aanvallen gestopt. Dingen zoals APOP voor POP accounts houden deze aanvallen tegen. (Normale POP logins zijn erg kwetsbaar voor dit, omdat alles Clear-text is wat over het net wordt gezonden.)

8.2 Systeem diensten en tcp_wrappers

Voordat je je Linux systeem op *ELK* netwerk zet, is het eerste waar je naar moet kijken welke diensten je moet aanbieden. Diensten die je niet moet aan bieden moeten worden uitgeschakeld zodat je een paar dingen minder hebt waar je je ongerust over moet maken en aanvallers hebben een paar plekken minder om aan te vallen en te zoeken naar een gat.

Er zijn een aantal manier om diensten onder Linux uit te schakelen. Je kan kijken in de `/etc/inetd.conf` file en kijk welke diensten worden aangeboden door je `inetd`. Schakel elke dienst uit die je niet nodig hebt door deze commentaar te maken (`#` op het begin van de regel), en zend dan je inetd proces een SIGHUP.

Je kan ook diensten verwijderen (of commentaar maken) in je `/etc/services` file. Dit betekend dat lokale clienten de service niet kunnen vinden (b.v, als je `ftp` weg haalt, en ze proberen te ftp-en naar een andere computer faalt het en zegt ünknown service"). Het is het niet waard om problemen te maken met het verwijderen van services, omdat het toch geen extra security met zich mee brengt. Als een lokale gebruiker `ftp` wil gebruiken zelfs als je het commentaar hebt gemaakt, maken ze hun eigen client die de normale FTP poort gebruikt en dan werkt het nog steeds goed.

Een van de diensten die je aan wilt laten staan zijn:

- `ftp`
- `telnet` (of `ssh`)
- mail, zoals `pop-3` of `imap`
- `identd`

Als je een bepaald pakket niet gaat gebruiken, kun je het gewoon helemaal verwijderen. `rpm -e` *`packagenaam`* onder de Red Hat distributie gooit het hele packet weg. Onder Debian doet `dpkg -remove` hetzelfde.

En, je kan je de rsh/rlogin/rcp uitzetten, en ook login (gebruikt door `rlogin`), shell (gebruikt door `rcp`), en exec (gebruikt door `rsh`) kun je uitzetten. Deze protocolen zijn extreem.

Je moet kijken in je `/etc/rc.d/rcN.d`, (waar `N` je systeem run level is) en kijk of een van de servers die in die directorie worden gestart onnodig zijn. De files in `/etc/rc.d/rcN.d` zijn eigenlijk gewoon symbolic links naar de directorie `/etc/rc.d/init.d`. De file hernoemen in de `init.d` directorie heeft als effect dat alle symbolische links worden uitgeschakeld in de `/etc/rc.d/rcN.d` directorie. Als je alleen een service wilt uitschakelen voor een bepaalde run level, hernoem dan de file door de grote `S` te vervangen met een kleine `s`, zoals dit:

```
root#  cd /etc/rc6.d
root#  mv S45dhcpd s45dhcpd
```

Als je BSD stijl `rc` files hebt, kun je `/etc/rc*` bekijken voor programma's die je niet nodig hebt.

De meeste Linux distributies leveren tcp_wrappers, die al je TCP diensten "verpakt". Een tcp_wrapper (`tcpd`) wordt gestart vanuit `inetd` ipv de echte server. `tcpd` checkt dan de host die een dienst aanvraagt, en dan de echter server uitvoert, of de toegang afwijst. `tcpd` stelt je instaat om toegang tot je diensten te ontzeggen. Je moet een `/etc/hosts.allow` maken en je moet de hosts invoeren die toegang moeten hebben tot de diensten die je computer bied.

Als je een thuis dailup gebruiker bent, geven we de suggestie om alles te denyen. `tcpd` logt ook alle mislukte pogingen om toegang te krijgen tot een dienst, zodat dit je kan waarschuwen als je wordt aan gevallen. Als je een nieuwe service toevoegt, moet je ze configureren om tcp_wrappers te gebruiken als ze TCP gebaseerd zijn. Bijvoorbeeld, een normale dail-up gebruiker kan vreemdelingen tegen houden als ze proberen te connecten naar je machine, maar je hebt nog steeds de mogelijkheid om mail te ontvangen, en netwerk connecties te maken naar het Internet. Om dit te doen, kunt je het volgende toevoegen aan j `/etc/hosts.allow`:

ALL: 127.

En natuurlijk je `/etc/hosts.deny` houdt in:

ALL: ALL

die externe connecties naar je machine tegenhoud, maar je kunt nog steeds van binnenuit connecties maken met servers op het internet.

Onthoud dat tcp_wrapper alleen diensten beschermd die gestart worden vanuit `inetd`, en een bepaald aantal andere. Er kunnen ook nog andere diensten draaien op je systeem. je kan `netstat -ta` gebruiken om een lijst te vinden van alle diensten die je machine aanbied.

8.3 Je DNS Informatie nakijken

Als je DNS informatie over alle computers in je netwerk goed bijhoud kan dit ook de security bevorderen. Als een onbevoegde host in je netwerk komt, kun je hem herkennen door het gebrek aan een DNS aangifte. Veel diensten kunnen worden geconfigureerd om connecties van computer die geen goede DNS aangifte heeft niet te accepteren.

8.4 `identd`

`Identd` is een klein programma dat normaal vanuit de `inetd` server draait. Het houdt bij welke Tcp diensten worden gebruikt, en geeft dit dan door aan degene die er om vroeg.

Veel mensen onderschatten de bruikbaarheid van `identd`, en daarom zetten ze het uit of blokkeren ze het voor de buitenwereld. `identd` is er niet om andere netwerken te helpen. Er is geen manier om te weten of de data die je krijgt van de `identd` van het andere netwerk correct is of niet. Er is geen bevestiging in `identd` aanvragen.

Waarom zou je het dan draaien? Omdat het *jou* helpt, en het is een ander data punt voor jouw in de opsporing. Als je `identd` niet is aangevallen, dan weet je dat het de andere netwerken verteld welke gebruikers of welk uid van mensen een TCP dienst draaien. Als de admin van een ander netwerk komt en je zeg dat er een van jouw mensen op zijn netwerk probeerde in te breken, kun je makkelijk actie ondernemen tegen die gebruiker. Als je `identd` niet draait moet je eerst een hoop log files doorkijken, om uit te vinden wie en wanneer het was, en normaal neemt dat een hele hoop tijd in beslag.

Het `identd` package dat geleverd wordt bij de meeste distributies heeft meer configuratie mogelijkheden dan veel mensen denken. Je kan het uitzetten voor een bepaalde gebruiker (ze kunnen een `.noident` file aanmaken), je kan alle `identd` aanvragen loggen (We raden dit aan), je kan een uid ipv de gebruikers naam laten weergeven of zelf NO-USER.

8.5 SATAN, ISS en andere netwerk scanners

Er zijn een aantal verschillende software packages om poort en dienst gebaseerd machines en netwerken te scannen. SATAN, ISS, SAINT en Nessus zijn een van de meest bekende. Deze software maakt verbinding met de doel computer (of alle doel machines op een netwerk) op alle poorten die ze kunnen, en dan proberen ze erachter komen wat er op die poort draait. Gebaseerd op deze informatie, kun jij vertellen of de machine zwak is en of deze misbruikt kan worden.

SATAN (Security Administrator's Tool for Analyzing Networks) is een poort scanner met een web interface. Het kan ingesteld worden om lichte, gemiddelde of zware onderzoeken uit te voeren op een machine of een netwerk van machines, en de problemen verhelpen die hij tegenkomt. Weet zeker dat je de kopie van SATAN van *metalab* `<http://metalab.unc.edu/pub/packages/security/Satan-for-Linux/>` haalt of van een betrouwbare Ftp of web site. Er is ook een Trojan van gemaakt en gedistributeerd op het web. *http://www.trouble.org/~zen/satan/satan.html*. Notitie: 'SATAN is al lang niet meer geupdate, en de tools hieronder kunnen misschien beter werk leveren.

ISS (Internet Security Scanner) is een andere poort scanner. Hij is sneller dan Satan, en kan dus beter zijn voor grote netwerken. Maar, SATAN geeft meer informatie.

Abacus is een packet van programma's voor host gebaseerde security en inbreuk detectie. Kijk op hun home page voor meer informatie. *http://www.psionic.com/abacus/*

SAINT is een recente versie van SATAN. Het is web gebaseerd en heeft meer tests van deze tijd dan SATAN. Je kan meer informatie vinden op: *http://www.wwdsi.com/saint*

Nessus is een gratis security scanner. Het heeft een GTK grafische interface voor gemakkelijk gebruik. Het is ook goed gemaakt voor hele goede plug-in setup voor het scannen van nieuwe poorten. Voor meer informatie kijk op: *http://www.nessus.org*

8.5.1 Poort scans detecteren.

Er zijn enkele tools gemaakt om je te waarschuwen voor onderzoeken door SATAN en ISS en andere scan programmatjes. Hoewel, liberaal gebruik van tcp_wrappers, en het vaak kijken naar je log files, kun je zulke dingen opmerken. Zelfs op de laagste instelling laat SATAN dingen achter in de logs van een Red Hat systeem.

Er is ook een "stealth"poort scanner. Een pakket met het TCP ACK bit ingesteld (gedaan als een connectie gerealiseerd is) zal door een packet-filtering firewall komen. Het terug kerende RST packet van een die _*had no established session*_ kan bewijzen dat deze poort open staat. Ik denk niet dat TCP wrappers dit detecteert.

8.6 `sendmail`, `qmail` en MTA's

Een de meest belangrijke diensten die je kunt aanbieden is een mail server. Ongelukkig, is het een van de makkelijkst aan te vallen diensten, simpel door het aantal taken die het moet uitvoeren en privileges het moet hebben.

Als je `sendmail` gebruikt is het erg belangrijk om altijd de nieuwste versie te hebben. `sendmail` heeft een lange historie van security misbruik. Wees er altijd zeker van dat je de nieuwste versie hebt van *http://www.sendmail.org.*

Onthoud dat sendmail niet hoeft te draaien voor jouw om mail te zenden. Als je een thuis gebruiker bent, kun je sendmail makkelijk geheel uitzetten, en simpel weg je mail client gebruiken om mail te zenden. Je kan er ook voor kiezen om de -bd"flag weg te halen uit de sendmail startup file, gewoon inkomende vragen voor mail uitschakelen. In andere woorden, je kan sendmail makkelijk zo vanuit het opstart script draaien:

```
# /usr/lib/sendmail -q15m
```

Dit zegt sendmail om de mail queue elke vijftien minuten leeg te gooien voor elk bericht dat niet van de eerste keer kon worden bezorgd.

Veel systeem administrators kiezen ervoor om sendmail niet te gebruiken, om gewoon een andere te gebruiken. Je kan overschakelen op `qmail`. `qmail` was ontworpen met security in de gedachten vanaf de grond af. Het is snel, stabiel, secuur. Qmail kan gevonden worden op *http://www.qmail.org*

In een directe competitie naar qmail is "postfix", geschreven door Wietse Venema, ook auteur van tcp_wrappers en andere security tools. Formeel genoemd vmailer, en gesponsord door IBM, is dit ook een mail transport agent geschreven vanaf de grond af met security in het achterhoofd. Je kan meer over vmailer vinden op *http://www.postfix.org*

8.7 Denial of Service Aanvallen

Een "Denial of Service"(DoS) aanval is een aanval waar de aanvaller probeert enkele bronnen het zo druk te laten hebben met het legitimeren van aanvragen, of het tegenspreken van gelegimiteerde gebruikers toegang tot je machine.

Denial of service aanvallen zijn veel toegenomen de laatste jaren. Een van de meest populaire en recente zijn staan hieronder. Notitie: Nieuwe komen te voorschijn, elke dag, dus dit zijn maar een paar voorbeelden. Lees de Linux security lijsten en de bugtraq lijst en archieven voor meer actuele informatie.

- **SYN Flooding** - SYN flooding is een 'network denial of service' aanval. Het maakt gebruik van een "loopholeïn de manier hoe TCP connecties maakt. De nieuwere Linux kernels (2.0.30 en hoger) hebben enkele configuratie opties om deze aanvallen tegen te houden. Zie 7 (Kernel Security) voor een overzicht van kernel protectie opties.
- **Pentium "F00F"Bug** - Het is pas ondekt dat een serie van codes gezonden naar een genuine Intel Pentium de computer rebooten. Dit betreft elke machine met een Pentium processor (geen clones, geen Ppro of PII) het maakt niet uit welk Operating systeem je draait. Linux kernel van 2.0.32 en hoger hebben een work around voor deze bug, dit houdt hen tegen om het systeem op slot te zetten. Kernel 2.0.33 heeft een verbeter versie van de kernel fix, en is voorgesteld voor versies boven de 2.0.32. Als je op een Pentium draait, moet je nu upgraden!
- **Ping Flooding** - Ping flooding is een simpel brute denial of service aanval. De aanvaller zend een överstroming"van ICMP pakketjes naar je machine. Als ze dit doen vanaf een computer met meer bandbreedte dan die van jou, kan je machine niet alles op het netwerk zenden. Een variant op deze aanval is genoemd "smurfing", zend ICMP pakketjes naar een computer met *je* machines terug keer IP. Dit stelt ze in staat om dit minder detecteer-baar te doen. Je kan meer informatie over de "smurf-aanval vinden op *http://www.quadrunner.com/~chuegen/smurf.txt* Als je ooit onder een ping flood aanval bent, gebruik dan een tool als `tcpdump` om te achterhalen waar de pakketjes vandaan komen (of waar ze vandaan lijken te komen), je kan contact met je provider opnemen met deze informatie. Ping floods kunnen makkelijk gestopt worden op de router laag of door het gebruik van een firewall.
- **Ping o' Death** - De Ping o' Death aanval zend ICMP ECHO REQUEST pakketjes die te groot zijn om in de kernel data structure te passen om ze op te slaan. Als je een enkele groot (65,510 bytes) "ping"packet naar hosts zendt zorgt ervoor dat ze vastlopen of zelfs crashen, deze is snel de "Ping o' Death"genoemd. Deze is al lang gefixt, en is al lang niets meer om je druk over te maken.
- **Teardrop / New Tear** - Een van de meest recente soort van misbruik. Die een bug misbruikt in de IP fragmentation code op Linux en Windows platformen. Het is gefixt in de kernel versie 2.0.33, en er hoeft geen extra optie geselecteerd te worden onder de compilatie. Linux is ook bestand tegen de "newtearäanval.

Je kan de code van de meeste exploits en een duidelijker beschrijving van hoe ze werken op *http://www.rootshell.com* vinden door hun zoek-machine te gebruiken.

8.8 NFS (Network File System) Security.

NFS is een erg wijd gebruikt file deel protocol. Het stelt servers die `nfsd` en`mountd` draaien om hun gehele filesysteem te ëxporteren"naar andere machines met NFS filesysteem ondersteuning in de kernel(of een andere soort client, als het niet linux is). `mountd` houdt bij welke file systemen er gemount zijn in `/etc/mtab`, en je kan ze bekijken met `showmount`.

Veel bedrijven gebruiken NFS om home directories aan gebruikers te geven, zodat het niet uit maak om welke machine ze inloggen in het cluster, ze hebben altijd hun eigen home files.

Er wordt maar een klein beetje security toegestaan in het exporteren van een filesysteem. Je kan de `nfsd` een andere root gebruiker (uid=0) laten omzetten naar de `nobody` gebruiker, zodat je hem de totale toegang tot files ontzegt. Hoewel, sinds individuele gebruikers (of op z'n minst met hetzelfde uid) toegang hebben to hun eigen files, kunnen ze naar hun eigen account su'en en zo hebben ze totale toegang tot de files. Dat is maar een kleine hindernis voor een aanvaller die je filesysteem kan mounten.

Als je NFS gebruikt, weet dan zeker dat je de files alleen exporteert naar de machines die het echt nodig hebben. Exporteer nooit je gehele root dir; exporteer alleen directories die je moet exporteren.

Zie de NFS HOWTO voor meer informatie over NFS verkrijgbaar op *http://metalab.unc.edu/mdw/HOWTO/NFS-HOWTO.html*

8.9 NIS (Network Information Service) (vroeger YP).

Network Information service (vroeger YP) is bedoeld om informatie te geven aan een groep machines. De NIS master bewaart de informatie tabellen en converteert ze in NIS map files. De maps worden dan verdeeld over het netwerk, dit stelt de NIS client in staat om hun login, pas-woord, home dir en shell informatie te geven (alle informatie in een standaard `/etc/passwd` file). Dit stelt de gebruiker in staat om hun pas-woord te veranderen en het zo door te voeren in het gehele NIS domein.

NIS is niet helemaal secure. Het is ook nooit bedoeld om veilig te zijn. Het is bedoeld om handig en bruikbaar te zijn. Iedereen die de naam van je NIS domein kan raden (waar ze ook zijn) kunnen een kopie krijgen van je passwd file en kunnen er zo "crackën "John the Ripperöp gebruiken om je pas-woorden uit te vissen. Het is ook mogelijk om NIS voor de gek te houden en zo enkele soorten van vervelende truukjes doen. Als je NIS moet gebruiken, wees dan gewaarschuwd voor de gevaren.

Er is een meer veilige vervanger voor NIS, genoemd NIS+. Kijk in het NIS HOWTO voor meer informatie: *http://metalab.unc.edu/mdw/HOWTO/NIS-HOWTO.html*

8.10 Firewalls

Firewalls zijn bedoeld voor het controleren van welke data in en uit je lokale netwerk mag. Meestal is de firewall computer verbonden aan het internet en aan je lokale LAN, en de enige manier om van je LAN naar het internet te komen is door de firewall. Op deze manier kan de firewall controleren wat wordt gestuurd en terug gestuurd vanaf het internet en je LAN.

Er zijn een aantal types van firewalls en methodes om ze in te stellen. Linux machines maken best goede firewalls. Firewall code kan gelijk in de kernel worden mee gebouwd vanaf kernel 2.0. `ipfwadm` voor 2.0 kernels, of `ipchains` voor 2.2 kernels, user-space programmaatjes geven je de mogelijkheid om de types data die je firewall toestaat aan te passen. Je kan ook specifieke types van netwerk verkeer laten loggen.

Firewalls zijn een erg bruikbare en belangrijke techniek in het beveiligen van je netwerk. Hoewel, je moet nooit denken dat als je een firewall hebt, je de machines erachter niet meer veilig hoeft te maken. Dit is een fatale fout. Kijk in de zeer goede `Firewall-HOWTO` voor meer informatie over firewalls. *http://metalab.unc.edu/mdw/HOWTO/Firewall-HOWTO.html*

Meer informatie kan ook worden gevonden in de IP-Masquerading mini-howto: *http://metalab.unc.edu/mdw/HOWTO/mini/IP-Masquerade.html*

Meer informatie over `ipfwadm` (De tool die je dingen laat veranderen aan je firewall, kan gevonden worden op hun home page: *http://www.xos.nl/linux/ipfwadm/*

Als je geen ervaring hebt met firewalls, en het plannen om er een op te zetten voor meer dan een simpele security politiek, is het Firewalls boek van O'Reilly and Associates of een van de andere online firewall documenten de moeite waard om te lezen. Kijk op *http://www.ora.com* voor meer informatie. Het Nationale Instituut van Standaarden en Technologie-en hebben een goed firewall document gemaakt. Het is gemaakt in 1995, maar is nog steeds best goed. Je kan het vinden op *http://csrc.nist.gov/nistpubs/800-10/main.html.* Ook van enige interesse kunnen zijn:

- Het Freefire Project – een lijst van vrij gebruikbare firewall tools, verkrijgbaar op *http://sites.inka.de/sites/lina/freefire-l/index_ en.html*

- SunWorld Firewall Design – geschreven door de auteurs van het O'Reilly boek, dit geeft een ruwe beschrijving van de firewall types. Het is verkrijgbaar op *http://www.sunworld.com/swol-01-1996/swol-01-firewall.html*

8.11 IP Chains - Linux Kernel 2.2.x Firewalling

Linux IP Firewalling Chains is een update voor de 2.0 Linux firewall code om de code van de 2.2 kernel te gebruiken. Het heeft een groot aantal nieuwe mogelijkheden , onder andere:

- Meer flexibele packet manipulatie
- Meer complexe accounting
- Kleine politiek veranderingen nu nog sneller
- Fragmenten kunnen nadrukkelijk worden tegengehouden, niet erkend, etc.
- Logt verdachte pakketjes.
- Kan andere protocolen aan dan ICMP/TCP/UDP.

Als je momenteel ipfwadm gebruikt op je 2.0 kernel, zijn er scripts verkrijgbaar die het converteren van ipfwadm naar ipchains.

Leest ook de IP Chains HOWTO voor meer informatie. Het is verkrijgbaar op *http://www.rustcorp.com/linux/ipchains/HOWTO.html*

8.12 VPN's - Virtual Private Networks

VPN's zijn een manier voor het creëren van een virtueel netwerk op een al bestaand netwerk. Dit virtuele netwerk is vaak versleuteld en passeert alleen verkeer naar de wezen die het netwerk die verbinding hebben gemaakt met het netwerk. VPN's worden vaak gebruikt om iemand te verbinden die thuis werkt met het bedrijfs netwerk door het gebruik van een encrypted virtueel netwerk.

Als een linux masquerading firewall gebruikt en je moet MS PPTP (Microsoft VPN point to point product) laten, is er een linux kernel patch om dat te doen. Zie *ip-masq-vpn*.

Er zijn verschillende VPN oplossingen verkrijgbaar:

- vpnd. Zie *http://www.crosswinds.net/nuremberg/˜anstein/unix/vpnd.html*.
- Free S/Wan, verkrijgbaar op *http://www.xs4all.nl/˜freeswan/*
- Ssh kan gebruikt worden om een VPN te creëren. Zie de VPN mini-howto voor meer informatie.
- vps (Virtual private server) op *http://www.strongcrypto.com*.

Zie ook de IPSEC sectie voor verwijzingen en meer informatie.

9 Security Preparatie (voordat je online gaat)

Ok, je hebt je systeem gecheckt, en je hebt vastgesteld dat het zo veilig mogelijk is, en je bent klaar om je computer online te zetten. Er zijn een aantal dingen die je nu moet doen om je voor te bereiden op een indringer, zodat je deze snel kan uitschakelen, en het zo weer terug draaiende te maken.

9.1 Maak een volledige Backup van je Machine

Discussies over backup methodes en opslag is buiten beschouwing van dit document, maar hier zijn een aantal woorden die te maken hebben met backups en security:

Als je minder dan 650mb data op een partitie hebt staan, is een CD-R kopie een goede manier (Om dat er later moeilijk mee te knoeien is, en als het er goed op staat kan het lang mee gaan). Tapes en andere re-writeable media moet write-protected zijn zo snel je backup klaar is. En leg ze dan op een veilige plaats zodat er niet mee geknoeid kan worden. Zorg dat je je backups maakt in een secure off-line gebied. Een goede backup laat je zeker weten dat je een goed iets hebt om je systeem van te herstellen.

9.2 Een goed Backup plan kiezen

Een zes-tape kringloop is makkelijk bij te houden. Dit houd in vier tapes voor de werkdagen, een tape voor de even Vrijdagen, en een voor de oneven Vrijdagen. Voor een periodieke backup uit bleke dag, en een volledige backup op de desbetreffende Vrijdag tape. Als je particuliere belangrijke veranderingen hebt gemaakt of belangrijke data hebt toegevoegd aan je system, een volledige backup kan dan handig zijn.

9.3 Backup Je RPM of Debian File Database

Na een inbraak kun je je RPM database gebruiken zoals je `tripwire` ook gebruikt, maar dan moet je wel zeker zijn dat deze niet veranderd is. Je moet je RPM database copieëren naar een floppy, en zorg dat deze copieëren altijd off-line gebeuren. De Debian distributie heeft ook zoiets.

DE files `/var/lib/rpm/fileindex.rpm` and `/var/lib/rpm/packages.rpm` zullen meestal niet op een floppy passen. Maar als ze ingepakt zijn, moet elk op een floppy passen.

Nu, als er op je systeem is ingebroken, moet je het volgende commando gebruiken:

```
root#  rpm -Va
```

om elke file op je filesysteem na te kijken. Zie de `rpm`, man page, om er meerdere opties aan toe te voegen zodat het niet zoveel laat zien. Onthoud dat je RPM binary niet veranderd mag zijn.

Dit betekend elke keer dat er een nieuwe RPM is toegevoegd aan het systeem dat de RPM database opnieuw moet worden gegenereerd. Je moet beslissen tussen de voordelen en nadelen.

9.4 Houd je Systeem Accounting data in de gaten

Het is erg belangrijk dat de informatie die van `syslog` komt niet is veranderd. De files in `/var/log` alleen leesbaar en schrijfbaar maken voor maar een bepaald aantal gebruikers is al een goed begin.

Houd een oogje op wat er daar wordt geschreven, vooral onder de `auth` faciliteit. Vele gefaalde logins, bijvoorbeeld, kunnen duiden op een poging tot inbraak.

Waar je moet kijken voor je log files hangt af van je distributie. In een Linux dat voldoet aan de "Linux Filesystem Standard", zoals Red Hat, kun je kijken in `/var/log` en kijk in `messages`, `mail.log`, en andere.

Je kunt meer vinden over waar je distributies alles logt door te kijken in je `/etc/syslog.conf` file. De file verteld waar `syslogd` (de syslog deamon) waar hij de verschillende berichten moet zetten.

Je kan ook je log-rotating scripts configureren om je log files langer te bewaren, zodat je meer tijd hebt om ze door te kijken. Kijk naar het `logrotate` package van een recente Red Hat distributie. Andere distributies hebben ook zulke processen.

Als er met je log files is geknoeid, zie dan of je kan achterhalen wanneer het gestart is, en met welke dingen er geknoeid zijn. Zijn er lange periodes van tijd die niet kunnen? Kijk dan naar je backup tapes (als je die hebt) voor on-verknoeide log files.

Log files worden vaak veranderd door een indringer om zijn sporen uit te wissen, maar ze kunnen nog steeds opgemerkt worden door rare gebeurtenissen. Je kan de indringer opmerken als deze toegang probeert te krijgen, of als deze een programma heeft misbruikt om root te worden. Je kan log files zien voordat de indringer ze heeft veranderd.

Je moet er ook altijd zeker van zijn dat je het `auth` gedeelte gescheiden houdt van de andere log data, o.a de pogingen om gebruiker te veranderen met `su`, login pogingen, en andere user accounting informatie.

Als het mogelijk is configureer je `syslog` zo dat het belangrijke informatie doorstuurt naar een andere computer. Dit houdt de indringer tegen om zijn sporen uit te wissen en zijn login/su/ftp/etc pogingen te wissen. Zie de `syslog.conf` man page, en kijk naar de `@` optie.

Er zijn een aantal meer uitgebreide `syslogd` programma's. Kijk op*http://www.core-sdi.com/ssyslog/* voor Secure Syslog. Secure Syslog stelt je instaat om je log entries te versleutelen en zo zeker te weten dat er niet mee geknoeid kan worden.

Een andere `syslogd` met meer mogelijk heden is *syslog-ng*. Het stelt je in staat om meer flexibiliteit toe toevoegen in het loggen van berichten en je kan ook je remote je data die je naar een andere computer stuurt beschermen tegen verknoeiing.

Tot slot, log files zijn veel minder bruikbaar als niemand ze leest. Maak altijd een beetje tijd vrij om naar je log files te kijken, om zo een gevoel te krijgen van hoe ze er op een gewone dag uitzien. Dit helpt om ab-normale situaties eruit te pikken.

9.5 Systeem Updates doen.

De meeste Linux gebruikers installeren vanaf een CDROM. Door de snelle natuur van security fixes, nieuwe (gerepareerde) programma's worden steeds maar uitgebracht. Voordat je je machine aan een netwerk verbindt, is het goed om op een goede FTP site de update's te gaan halen. Vaak houden ze een belangrijke security reparatie in, dus is het een goed idee ze te installeren.

10 Wat te doen Tijdens en na een Inbraak

Dus je hebt enkele van de adviezen hier(of ergens anders) opgevolgd en je hebt een inbraak gedetecteerd? Het eerste wat je moet doen is kalm blijven. Haastige acties kunnen meer schade veroorzaken dan de aanvaller wilde hebben.

10.1 Een Security aanval is bezig

Een Security aanval detecteren kannen een spannende ondernemening zijn. Hoe je reageert kan grote consequenties hebben.

Als de aanval die je ziet een fysieke is, is er een grote kans dat er iemand in je huis heeft in-gebruiken, je kantoor of lab. Je moet je lokale autoriteiten waarschuwen. In een lab, kun je iemand opgemerkt hebben die een computer probeert te rebooten of een kist probeert te openen. Gebaseerd op je bevoegdheden en procedures, kun je ze vragen om hem te stoppen, of je kun je lokale security mensen bellen.

Als je detecteert dat een lokale gebruiker je security probeert te doorbreken is het eerste wat je doet kijken of het de gene is wie je denkt dat het is. Kijk op het netwerk waarvan ze zijn in-gelogd. Is het de manier hoe ze normaal inloggen? Nee? Gebruik dan een niet elektronische manier om in contact te komen. Bijvoorbeeld, bel ze of loop naar hun kantoor of huis en praat tegen ze. Als ze toegeven dat zij het waren, kun je ze vragen om uit te leggen wat ze gedaan hebben en of ze daar mee willen stoppen. Als ze het niet weten, en ze hebben geen idee waar je over praat, vraagt het om een uitgebreider onderzoek. Kijk naar zulke incidentjes en zorg dat je veel informatie hebt voordat je iemand beschuldigt.

Als je een netwerk aanval hebt gedetecteerd, is het eerste wat je doet (als je kunt) het netwerk afbreken. Als ze verboden zijn met een modem trek dan de stekker van de modem eruit; Als ze via het ethernet komen, trek dan die kabel eruit. Dit stopt ze om nog meer schade aan te richten, en ze zullen het zien als een netwerk probleem, in plaats van detectie.

Als het onmogelijk is om het netwerk af te sluiten (je hebt een druk bedrijf, je hebt geen fysieke control over je machines), is de beste stap een programma als `tcp_wrappers` of `ipfwadm` te gebruiken om het netwerk waar de indringers vandaan komen de toegang te ontzeggen.

Als je niet alle mensen van het zelfde netwerk als de indringers kan tegenspreken, moet je het gebruikers account op slot zetten. Een account opslot zetten is niet gemakkelijk. Je moet rekening houden met de `.rhosts` file, FTP toegang, en een mogelijke achterdeur.

Als je een van de dingen hierboven hebt gedaan (het netwerk afsluiten, toegang ontzeggen van hun netwerk, en/of hun account uitschakelen), moet je al hun gebruikers processen killen en hun uitloggen.

Je moet je netwerk een aantal minuten goed in de gaten houden, als de aanvallers terug proberen binnen te komen. Bijvoorbeeld op een ander account en/of van een ander netwerk-adres.

10.2 De security aanval is al geweest

Dus je hebt een pas een aanval gedetecteerd die al is gebeurt of je hebt er een gedetecteerd en de aanvaller uit je systeem gezet (hopelijk). En nu?

10.2.1 Het gat dichten

Als je kan achterhalen hoe de aanvaller is binnengekomen in je systeem, moet je het gat proberen te dichten. Bijvoorbeeld, je ziet enkele FTP aangifte's in je log files vlak voordat de aanvaller is in-gelogd. Schakel dan FTP uit en kijk of er een nieuwe versie.

Bekijk alle logfile's, en ga op bezoek bij je security lijst en pagina's en kijk of er nieuwe algemeen misbruik is wat je kan repareren. Je kan de Caldera security fixes vinden op *http://www.caldera.com/tech-ref/security/*. Red Hat heeft de security fixes nog niet gescheiden van de bug fixes, maar hun distributie errata is verkrijgbaar op *http://www.redhat.com/errata*

Debian heeft nu een security mailing list en een web-page Zie: *http://www.debian.com/security/* voor meer informatie.

Het is zeer gebruikelijk als een van de lever een security update uitbrengt, dat de meeste andere dat dan ook doen.

Er is nu een linux security boekhouding project. Er komen methodes om alle user space utilities om te kijken voor een mogelijke security misbruik of een overflow. Uit hun aankondiging:

> "We pogen een systematische boekhouden van de Linux sources te maken met als doel zo veilig worden als Open-BSD. We hebben al enkele problemen ontdekt (en opgelost), maar meer hulp is welkom. De lijst is oncontroleerbaar en is een bruikbare bron voor algemene security discussies. Het adres van de lijst is: security-audit@ferret.lmh.ox.ac.uk Om je in te schrijven moet je een mailtje zenden naar: security-audit-subscribe@ferret.lmh.ox.ac.uk"

Als je de aanvaller niet buiten zet, zullen ze terug komen. Niet alleen terug op jouw machine, maar terug ergens op je netwerk. Als je een packet sniffer draaiden, onveiligheden zijn voor hen goed om naar andere lokale machines te gaan.

10.2.2 De schade schatten

Het eerst dat je doet om de schade in te schatten is. Wat is er aangevallen? Aks je een Intergeriteit Checker als `Tripwire` draait, kun je het gebruiken om een integeriteits check uit te voeren, en dat kan je helpen om de schade vast te stellen. Als het niet help, moet je rond kijken naar de belangrijke data.

Sinds Linux system makkelijker en makkelijker te installeren zijn, kun je je configuratie files op een diskketje('s) zetten en het zo her installeren, dan je gebruikers files van ja backups herstellen. Dat laat je zeker weten dat je weer een schoon systeem hebt. Als je files moet backup-en van een binnengedrongen systeem, kan gevaarlijk zijn zeker met binaries, omdat ze een Trojan horse kunnen zijn geplaatst door een indringer.

Re installatie moet verplicht gesteld worden als de de indringer root toegang heeft gehad. Maar, je kan wel het bewijs materiaal bewaren, dus als je een reserve disk hebt kan een goede gedachte zijn.

Dan moet je je druk maken over hoe lang geleden de aanval is gebeurd, en of de backups beschadigd werk bevatten. Meer over backups later.

10.2.3 Backups, Backups, Backups!

Als je een reguliere backup hebt is een geschenk van god voor security. Als je systeem is binnen gedrongen, kun je de data die je nodig hebt herstellen van een backup. Natuurlijk, sommige data is waardevol voor een aanval, en ze zullen het niet alleen kapot maken, ze stelen het en hebben hun eigen copieëren maar je hebt nog steeds de data.

Je moet enkele backups terug checken voordat je de verknoeide file het hersteld. De indringer kan de files een tijdje geleden hebben verknoeid, en je kan enkele succesvolle backups hebben gemaakt van de verknoeide file!!!!

Natuurlijk, er zijn ook een aantal security bezorgd-heden met backups. Zorg dat je ze op een veilige plaats bewaard. Weet wie toegang tot ze heeft. (Als een aanvaller je backups kan pakken, kunnen ze toegang hebben tot al je data zonder dat je het weet.)

10.2.4 De indringer terug vinden.

Ok, je hebt de indringer van je systeem geschopt, en je systeem hersteld, maar je bent nog niet klaar. Zolang het niet waarschijnlijk is dat de indringer wordt gepakt, moet je de aanval toch aangeven.

Je moet de aanval aangeven bij de admin van het netwerk waar de indringer vandaan kwam. Je kan zijn adres opvragen met `whois` of de Internic database. Je kan ze een email zenden met alle log entries en datum's en tijden. Als je iets anders strafbaars tegen komt over de indringer moet je dat ook melden. Na dat, moet je (als je zo Be-invloed bent) ook bellen. Als de desbetreffende admin de aanvaller vindt, kun je met de admin praten over waar ze vandaan komen en zo.

Goede krakers gebruiken vaak tussen liggende systemen, enkele (of veel) van welke ze niet weten dat ze zijn binnen gedrongen. Dan het adres van de kraker vinden kan moeilijk zijn. Door beleefd te zijn tegen de admin's kan ook helpen om hulp van hem te krijgen.

Je moet ook een security organisatie waar je deel van bent waarschuwen (*CERT* `<http://www.cert.org/>` of een andere), en ook je Linux systeem dealer.

11 Security Bronnen

Er zijn een HOOP goede sites voor Unix security in het algemeen en Linux security gespecificeerd. Het is erg belangrijk om je in te schrijven bij on (of meer) van de security mailing lists om je op de hoogte te houden van de security fixes. Veel van deze lijsten zijn erg informatief.

11.1 FTP Sites

CERT is de Computer Emergency Response Team. Ze zenden vaak een alarm van de actuele aanvallen en fixes. Zie *ftp://ftp.cert.org* voor meer informatie.

Replay (*http://www.replay.com*) heeft archieven van veel security programma's. Sinds ze buiten de VS zitten, hebben ze geen last van de VS crypto beperkingen.

Matt Blaze is de schrijver van CFS en een goede security advocaat. Matt's archief is verkrijgbaar op *ftp://ftp.research.att.com/pub/mab* `<ftp://ftp.research.att.com/pub/mab>`

`tue.nl` is een goede security FTP site in Nederland. *ftp.win.tue.nl*

11.2 Web Sites

- De Hacker FAQ is een FAQ over hackers: *De Hacker FAQ*
- Het COAST archief heeft een groot aantal Unix security programma's en informatie: *COAST*
- SuSe Security Pagina: *http://www.suse.de/security/*
- Rootshell.com is een geweldige site om te zien welke soorten misbruik er nu worden gebruikt door crackers: *http://www.rootshell.com/*
- BUGTRAQ geeft advies over security onderwerpen: *BUGTRAQ archieven*
- CERT, het Computer Emergency Response Team, geeft advies over gebruikelijke aanvallen op unix platformen: *CERT home*
- Dan Farmer is de auteur van SATAN en vele andere security tools. Zijn home page heeft enkele interessante security verslagen en ook security tools: *http://www.trouble.org*
- De Linux security WWW is een goede site voor Linux security informatie: *Linux Security WWW*
- Infilsec heeft een zwakheids motor die je kan vertellen welke zwakheden met welk platform te maken hebben: *http://www.infilsec.com/vulnerabilities/*
- CIAC zend periodieke security bulitins over algemeen misbruik: *http://ciac.llnl.gov/cgi-bin/index/bulletins*
- Een goed startpunt voor de Linux Pluggable Authentication modules kan gevonden worden op *http://www.kernel.org/pub/linux/libs/pam/*.
- Het debian project heeft een web page voor hun eigen security fixes en informatie. Het is te vinden op *http://www.debian.com/security/*.
- WWW Security FAQ, geschreven door Lincoln Stein, is een geweldige web site met security verwijzingen. Te vinden op *http://www.w3.org/Security/Faq/www-security-faq.html*

11.3 Mailing Lists

Bugtraq: Om je in te schrijven voor bugtraq, zend een mailtje naar listserv@netspace.org met in de body subscribe bugtraq. (zie de links boven de archieven).

CIAC: Zend een mailtje naar majordomo@tholia.llnl.gov. In de BODY (niet het subject) van het bericht: subscribe ciac-bulletin

Red Hat heeft een aantal mailing lists, de belangrijkste is de redhat-annouce lijst. Je kan lezen over security (en andere) fixes zo snel ze uitkomen. Zend een mailtje naar majordomo@redhat.com en zet erin subscribe redhat-announce.

Het Debian project heeft een security mailing list die hun fixes inhoud. zie *http://www.debian.com/security/* voor meer informatie.

11.4 Boeken - Geprint materiaal

Er zijn een aantal goede security boeken. Deze geeft een lijst van een aantal van deze. Als toevoeging op security specifieke boeken, zijn er ook boeken over systeem administratie waar ook een beetje over security in staat.

Building Internet Firewalls By D. Brent Chapman & Elizabeth D. Zwicky

1st Edition September 1995

ISBN: 1-56592-124-0

Practical UNIX & Internet Security, 2nd Edition By Simson Garfinkel & Gene Spafford

2nd Edition April 1996

ISBN: 1-56592-148-8

Computer Security Basics By Deborah Russell & G.T. Gangemi, Sr.

1st Edition July 1991

ISBN: 0-937175-71-4

Linux Network Administrator's Guide By Olaf Kirch

1st Edition January 1995

ISBN: 1-56592-087-2

PGP: Pretty Good Privacy By Simson Garfinkel

1st Edition December 1994

ISBN: 1-56592-098-8

Computer Crime A Crimefighter's Handbook By David Icove, Karl Seger & William VonStorch (Consulting Editor Eugene H. Spafford)

1st Edition August 1995

ISBN: 1-56592-086-4

12 Lijst van begrippen

- **bevestiging:** De eigenschap om te kijken of de data die gezonden is het zelfde is als de data die is gezonden, en dat de gene die zegt dat hij de zender is ook de echte zenden is.

- **bastion Host:** Een computer systeem dat heel veilig moet zijn, omdat het zwak is voor aanvallen, meestal omdat deze is blootgelegd aan het Internet en een algemeen punt is van gebruikers van de interne netwerken. Het heeft zijn naam te danken aan de hoge versterkte projecten aan de buitenste muren van middeleeuwse kastelen. Bastions overzien kritiek gebieden van verdediging, meestal omdat ze sterke muren hebben, ruimte voor extra troepen, en een en een tijdelijke tobbe van kokend hete olie voor het afschrikken van de aanvallers.
- **buffer overflow:** Normale coding style is nooit goed om groot genoege buffers te maken, en om niet te checken voor overflows. Als zulke buffers overspoelen, kan het uitgevoerde programma (deamon of set-uid programma) gedwongen worden om iets anders te gaan doen. Normaal werkt dit door het overschrijven van een functie's return address op de stack om naar een andere lokatie te wijzen.
- **denial of service:** Een denial of service attack is wanneer een aanvaller de bronnen van je computer op eet voor dingen die het niet behoort te doen, dus normale gebruikers tegenhouden om hun netwerk te gebruiken voor eigen doelen.
- **dual-homed Host:** Een gewone computer die op z'n minst twee netwerk kaarten heeft.
- **firewall:** Een component of een aantal componenten die toegang ontzeggen tussen een beschermd netwerk en het Internet, of tussen een aantal andere netwerken
- **host:** Een computer aangesloten op een netwerk.
- **IP spoofing:** IP Spoofing is een complexe techniek van aanvallen dat opgebouwd is uitverschillende componenten. Het is een security aanval dat werk door te doen of je een vertrouwde computer bent, maar je bent het niet. Er zijn dure stukken geschreven door deamon9, route, en infinity in het Volume Seven, Onderwerp 48 onderwerp van Phrack Magazine.
- **non-repudiation:** Het bezit van een zender om te bewijzen dat hij het heeft gezonden ook al ontkent hij dat.
- **packet:** De fundemantele eenheid van communicatie over het Internet.
- **packet filtering:** De actie die een device maakt om selectief de stroom van data naar en van het netwerk te controleren. Packet files staan pakketjes toe of wijzen ze of, gebruikelijk wanneer ze worden door gestuurd van het ene naar het andere netwerk. (Meestal vanaf het Internet naar het interne netwerk, en andersom). Om packet filtering te voltooien, moet je regels instellen die aangeven welk type packet wordt binnen gelaten (die van of naar een particulier IP adres of poort) en welk niet.
- **perimeter network:** Een network toegevoegd tussen een beschermd netwerk en een extern netwerk, om een extra laag van security aan te brengen. Een perimeter netwerk wordt soms een DMZ genoemd.
- **proxy server:** Een programma dat handelt met de externe servers in plaats van de interne clienten. Proxy clienten praten tegen een proxy server, welke de aanvragen door sturen naar de echte servers, en het antwoord doorsturen naar de clienten.
- **superuser:** Een informele naam voor `root`.

13 Frequently Asked Questions

1. Is het veiliger om een driver in de kernel te compileren dan er een module van te maken? Antwoordt: sommige mensen denken het beter is om het laden van modules uit te schakelen om drivers te laden, omdat een inbreker een Trojan module of een andere module die de security van het systeem kan ondermijnen laden.

Alhoewel je root moet zijn om modules te laden. De module object files zijn ook enkel over-schrijfbaar door de root. Dit betekend dus dat de inbreker root priveleges nodig heeft om een module te laden. Als de inbreker eenmaal root priveleges heeft dan zijn er serieuzere dingen om je zorgen over te maken i.p.v. de modules die hij wil laden

Modules zijn voor het dynamisch laden van support voor een willekeurige devices die misschien zelden wordt gebruikt. Op server machines, of firewalls bijvoorbeeld is dit niet echt gewenst. Om deze redenen is het beter de support direct in de kernel mee te compileren. Modules zijn ook langzamer dan support direct in de kernel mee gecompileerd.

2. Waarom mislukt altijd het inloggen als root van remote machineas ? Antwoord: Zie 4.2 (Root Security). Dit is opzettelijk gedaan om remote gebruikers die en poging doen om te connecten met `telnet` naar jou machine als `root`, wat zeer onveilig is. Vergeet niet: Dat potentiele inbrekers de tijd hebben, en programma's hebben om jou pas-woord te vinden.

   De `/etc/passwd` file wordt dan gebruikt om gebruikers en groepen Namen op te slaan, gebruikt door programma's zoals `/bin/ls` om het gebruikers nummer om te zetten in een gebruikers naam bij een directory uitvoer.

   De `/etc/shadow` file bevat enkel de gebruikersnaam en zijn/haar pas-woord, en misschien andere accounts gegevens zoals wanneer het account vervalt enz.

   Om shadow passwords mogelijk te maken run dan `pwconv` als root en `/etc/shadow` bestaat nu als het goed is en wordt gebruikt door applications. Sinds RH 4.2 en daar boven, worden de PAM modules automatisch aangepast voor het gebruik van `/etc/passwd` naar de shadow passwords zonder iets anders te veranderen.

   Sinds je belangstelling in het beveiligen van je pas-woorden, misschien heb je dan ook interesse in het maken van goede pas-woorden. Voor dit kun je gebruik maken van `pam_cracklib` module, welke een stukje is van PAM. Het draait je pas-woord tegen een Crack bibliotheek om je te helpen met het besluiten of je pas-woord makkelijk raadbaar is.

3. Hoe kan ik in Apache SSL extensies aanzetten? Antwoord:

   1.Haal SSLeay 0.8.0 of later van `<ftp://ftp.psy.uq.oz.au/pub/Crypto/SSL>`

   2.Bouw, test en installeer het!

   3.Haal de Apache 1.2.5 source

   4.Haal Apache SSLeay extensies van *ftp://ftp.ox.ac.uk/pub/crypto/SSL/* `<ftp://ftp.ox.ac.uk/pub/crypto/SSL/apache_1.2.5+ssl_1.13.tar.gz>`

   5. Pak het uit in de apache-1.2.5 source directorie en patch Apache als in de README.

   6.Configureren en bouwen.

   Je kan ook *Replay Associates* proberen welke vele voor gebouwde pakketjes heeft en is gelocaliseerd buiten de VS.

4. Hoe kan ik gebruikers accounts manipuleren, en ook mijn security bewaren? Antwoord: De Red Hat distributie, vooral RH5.0, hebben een groot aantal tooltjes om de instellingen van gebruikers accounts te veranderen.

   - De `pwconv` en `unpwconv` programma's kunnen worden gebruikt voor het converteren tussen shadow en non-shadowed pas-woorden.
   - De `pwck` en `grpck` programma's kunnen worden gebruikt om de organisatie van de `passwd` en `group` files te verificeren.
   - De `useradd`, `usermod`, en `userdel` programma's kunnen worden gebruikt om gebruikers account toe te voegen, te verwijderen of te veranderen. De `groupadd`, `groupmod`, en `groupdel` programma's doen het zelfde maar dan voor groepen.

- Groep pas-woorden kunnen worden gecreerd door het gebruik van `gpasswd`.

Alle programma's zijn "shadow-aware-- dit is, als je schadow inschakeld gebruiken ze `/etc/shadow` voor pas-woord informatie, anders niet.

Zie de respectievelijke man pagina voor meer informatie.

5. Hoe kan ik sommige HTML documenten beschermen met Apache? I wet dat je *http://www.apacheweek.org* niet kende, of wel?

   Je vindt meer informatie over gebruikers verificatie op *http://www.apacheweek.com/features/userauth* ook op de web server security tips van *http://www.apache.org/docs/misc/security_tips.html*

14 Conclusie

Door je in te schrijven op een security alert mailing list, en je systeem up to date houden, kun je een hoop doen om je systeem veilig te houden. Als je aandacht besteed aan je log files en je draait geregeld iets als `tripwire`, kun je nog meer doen.

Een redelijke laag van computer veiligheid is niet moeilijk te onderhouden op een thuis machine. Meer moeite is er nodig op een bedrijfs machine, maar Linux kan een zeer veilig platform zijn. Doordat Linux veel ontwikkeld wordt komen veiligheids reparaties vaak sneller als bij commerciele Operating systems, dat maak Linux een ideaal platform als Security nodig is.

15 Erkentenis


```
Informatie hier is bij elkaar gehaald uit vele bronnen. Dank aan
de volgende die indirect of direct hebben mee geholpen:
```

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.soltc.net*

David S. Jackson *dsj@dsj.net*

Todd G. Ruskell *ruskell@boulder.nist.gov*

Rogier Wolff *R.E.Wolff@BitWizard.nl*

Antonomasia *ant@notatla.demon.co.uk*

Nic Bellamy *sky@wibble.net*

Eric Hanchrow *offby1@blarg.net*

Robert J. Berger*rberger@ibd.com*

Ulrich Alpers *lurchi@cdrom.uni-stuttgart.de*

David Noha *dave@c-c-s.com*

De volgende hebben de howto vertaald in verschillende andere talen!

Een speciale dank aan hun allen voor het helpen verspreiden van het linux woord...

Pools: Ziemek Borowski *ziembor@FAQ-bot.ZiemBor.Waw.PL*

Japans: FUJIWARA Teruyoshi *fjwr@mtj.biglobe.ne.jp*

Indonesies: Tedi Heriyanto *22941219@students.ukdw.ac.id*