Hur du gör din Linuxdator säkrare

Av: Kjell Enblom, Cendio Systems AB
December 2001

Presentationen finns även på: http://www.lysator.liu.se/upplysning/

Innehåll:

Introduktion till säkerhet

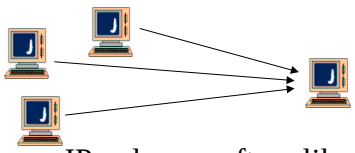
- I säkerhetssammanhang talar man om
  - sekretess
    - Sekretess innebär att obehöriga inte får komma åt information som de inte ska ha tillgång till.
  - integritet
    - Integritet är att ingen obehörig ändrar på data.
  - tillgänglighet
    - Tillgänglighet innebär att de som ska ha tillgång till data får komma åt data.

Introduktion till säkerhet

- Även om du tycker att din dator inte har någonting viktigt eller hemligt på sig måste du skydda den.
- Din dator kan användas som språngbräda i attacker mot andra.
- Det är bara en tidsfråga innan du kommer att utsättas för en eller flera attacker.
- Skräckexempel är nyinstallerade datorer som har blivit attackerade efter mindre än en timma.
  - Intrång har skett under fikapaus efter installation.

Olika typer av attacker

- Attacker finns av många olika typer. Här går vi igenom några av de vanligaste.
  - DoS, DDoS, förhindrande av en tjänst. Kan till exempel vara ett nät som kloggas igen eller en server som överlastas. DDoS är en distribuerad form av DoS-attack där många datorer eller nät attackerar ett mål.

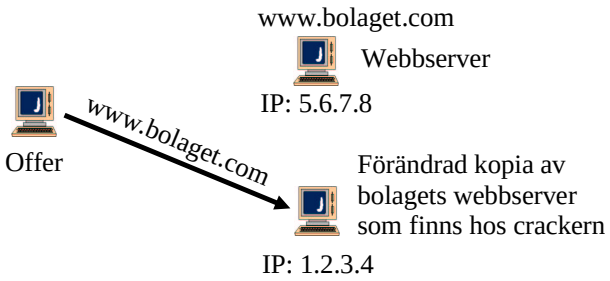


  - Scanning av IP−adresser efter olika typer av servrar. T.e.x. scanna stora nätverk efter IIS−servrar eller wu−ftpd.

Olika typer av attacker

- Buffer overflow, att skicka mer data än vad det ska vara. Många program kontrollerar inte att data de får är korrekta.
- Fragmenterade paket. Kan till exempel vara överlappande fragment.
- Brytande mot standarder. Ett exempel kan vara att skicka både uppkopplingsbegäran (SYN) och nedkopplingsbegäran (FIN) samtidigt.
- DNS−förgiftning för att till exempel få offret att gå till en annan server (attackerarens). Ett exempel på en sådan attack är den som sourceforge drabbades av i somras.

Olika typer av attacker
DNS−förgiftning



Offret luras här att surfa till fel webb−server.

Olika typer av attacker

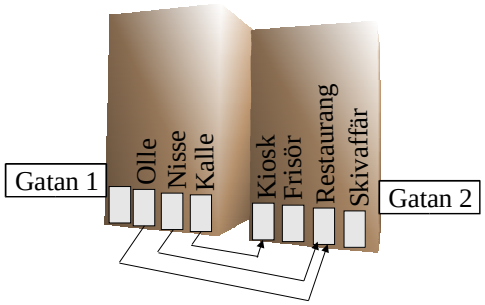
- Maskar, program som utnyttjar buggar i servertjänster och som bryter sig in på servrarna och därifrån attackerar nya servrar. Exempel på maskar är Lionworm, Ramen, Code Red, W32/Nimda−A.
- Virus, program som infekterar andra program och filer. Tack och lov inte särskilt vanligt i Linuxvärlden.
- Trojanska hästar, program som inte bara gör det de ska utan som även har destruktiva funktioner inbyggda.
  - Kan på ytan se ut som ett bra nyttoprogram.
  - Kan vara en fixad kopia av ett nyttoprogram (ungefär som ett virussmittat program).

Olika typer av attacker

- Crackers samlar på information om IP−adresser och vilka servrar som körs på dessa. Informationen kan sedan sparas i en databas och utnyttjas vid ett senare tillfälle utan att behöva göra en ny scanning.
- Vid intrång installeras ofta program för att dölja intrånget. Program byts ut, logfiler rensas från bevis.
  - Exempel: ps, ls, finger, who, ifconfig, route byts ut mot ”egna versioner” för att gömma filer, processer, inloggade användare etc. .

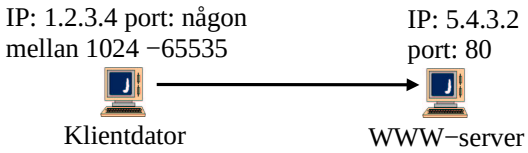
Kort introduktion till nät

- I nätverkssammanhang används förutom IP−adresser även portar.
  - En förbindelse består av avsändaradress, avsändarport och mottagaradress, mottagarport.



Kort introduktion till nät

- I datornät finns oftas servertjänsterna på kända portar.
  - ssh, port 22
  - e−postservrar, port 25
  - WWW−servrar, port 80
  - pop3, port 110
- En webbuppkoppling kan se ut enligt följande:



Några nätverkstjänster och säkerhetsaspekter på dessa

- Många nätverkstjänster skickar data i klarttext över nätet.
- Ett nätverk är mycket enkelt att avlyssna och därmed trafiken på nätet.
- Många tjänster skickar användarnamn och lösenord i klartext. Undvik att använda dessa.

Några nätverkstjänster och säkerhetsaspekter på dessa

- Exempel på nätverkstjänster som skickar data i klartext:
  - Telnet (terminaluppkoppling)
  - rsh, rlogin (för att köra kommandon remote)
  - WWW
  - E−post (SMTP, POP, IMAP)
  - FTP (filöverföring)
  - DNS (namn− och IP−nummeruppslagningar)

Några nätverkstjänster och säkerhetsaspekter på dessa

- Exempel på krypterade förbindelser:
  - ssh (terminalförbindelse, kan även användas för att tunnla annan trafik)
  - Kerberos (terminalförbindelser och annan trafik)
  - SSL (för bland annat säker webbtrafik, https)
- Kryptera och signera alltid känslig information som skickas med e−post.
  - Använd till exempel PGP eller GPG.

Förebyggande åtgärder

- Kontrollera vilka servertjänster som körs på din dator. Några användbara kommandon till det är:
  - lsof −i
  - netstat −a
- Alla servertjänster som du inte vet vad de är för några ska stängas av.
- Det gör ingenting om för mycket stängs av. Det är enkelt att slå på en servertjänst igen.

Förebyggande åtgärder

- Nätverksservertjänster kan startas på två sätt:
  - genom ett program som lyssnar på uppkopplingar åt dem (inetd eller xinetd).
  - med hjälp av ett skalprogram som startar dem vi boot.

inetd/xinetd

- inetd använder konfigurationsfilen /etc/inetd.conf
- xinetd använder en fil för varje tjänst där filerna ligger i /etc/xinetd.d/
- Stäng av alla tjänster som du inte använder.
  - I inetd.conf kommenterar du bort tjänsten med # i början av raden för den aktuella tjänsten.
  - För xinetd sätter du i filen för varje tjänst som ska stängas av:
    - disable = yes

inetd/xinetd

- Starta sedan om inetd respektive xinetd med:
  - killall -HUP inetd
  - killall -HUP xinetd.

Övriga servertjänster

- För övriga servertjänster radera filerna (symlänkarna) i katalogerna för de run levels du vill ta bort servertjänsten.
  - Exempel: rm /etc/rc3.d/S45tjänst
  - Exempel, RPM−baserad Linux: chkconfig tjänst off
  - Exempel, RPM−baserad Linux: ntsysv
  - I slackware får du kommentera bort servertjänsterna i /etc/rc.d/rc.inet2

Uppgradering

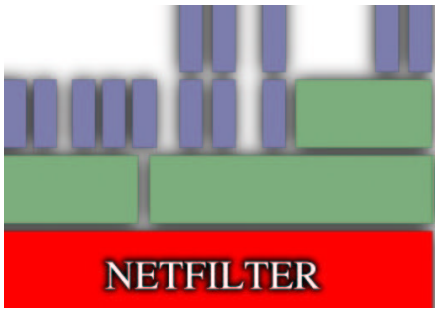
- Se alltid till att uppgradera de servertjänster du kör så att de kör den senaste säkra versionen.
- Byt ut wu-ftpd mot någon säkrare ftp−server (exempel portning av openBSD:s ftp−server).

Brandväggsskydd

- Säkra upp dina datorer med brandväggsskydd.
  - 2.0−kärnor kör ipfwadm
  - 2.2−kärnor kör ipchains
  - 2.4−kärnor kör netfilter/iptables

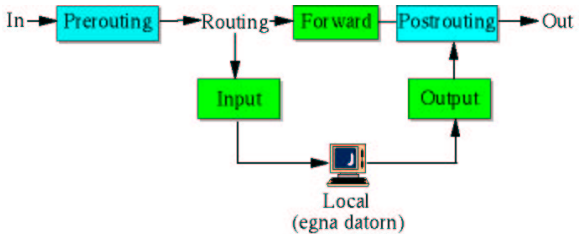
Netfilter/iptables

- I 2.4−kärnor finns netfilter som är själva brandväggsstödet. Ovanpå netfilter körs sedan iptables, adressöversättning etc.



Netfilter/iptables

- Netfilter består av ett antal kedjor, routingval och adressöversättning.
- Trafiken till den egna datorn går via Input.
- Trafiken ut från den egna datorn via Output.



Netfilter/iptables

- Trafik från ett nätverkskort till ett annat passerar Forward.
- Prerouting gör adressöversättning på mottagaradress.
- Postrouting gör adressöversättning på avsändaradress.

Kärnmoduler

- Om allt brandväggsstöd ligger fast inkompilerat i kärnan behövs inga moduler laddas.
- Om brandväggsstödet ligger som moduler till kärnan måste dessa laddas först innan de kan användas.
- En modul laddas med:
  - modprobe modulen
- Inladdade kärnmoduler listas med:
  - lsmod

Kärnmoduler

- Exempel på moduler:
  - **ip_conntrack** håller reda på förbindelser.
  - **ip_conntrack_ftp** håller reda på ftp−förbindelser.
  - **iptable_filter** gör att det går att kasta, spärra och logga trafik.
  - **iptable_nat** modul för maskering.
  - **ip_nat_ftp** modul för maskering av ftp−trafik.

Introduktion till brandväggsregler

- De flesta tjänster använder TCP.
  - För TCP−förbindelser behövs en brandväggsregel för uppkopplingstrafiken och en för svarstrafiken.
- Tjänster som skickar mycket små datamängder eller som skickar dataströmmar (ljud, video) använder oftast UDP.
  - UDP använder inte uppkopplingar utan skickar bara data.
  - För UDP−baserad trafik behövs två brandväggsregler, en för data i vardera riktning.

Introduktion till brandväggsregler

- ICMP används för att skicka meddelanden som t.ex. felmeddelanden om nät och datorer som inte är nåbara.
- Ut från den egna datorn vill man oftast inte begränsa trafiken. För utgående trafik (Output) sätter vi upp brandväggsregler som släpper fram allt.
- In till den egna datorn ska bara några få tjänster vara nåbara och där ska allt utom trafik till dessa tjänster spärras.

Brandväggsregler

- Börja med att sätta upp standardregler.
  - /sbin/iptables -P INPUT DROP
  - /sbin/iptables -P OUTPUT ACCEPT
  - /sbin/iptables -P FORWARD DROP
- Rensa bort gamla regler och kedjor.
  - /sbin/iptables -F
  - /sbin/iptables -X
- Det enda som finns nu är standardreglerna.

Brandväggsregler

- Definiera en egen kedja, logdrop, som loggar och kastar trafik.
  - /sbin/iptables -N logdrop
  - /sbin/iptables -A logdrop -j LOG
  - /sbin/iptables -A logdrop -j DROP
- Den nya kedjan kan nu användas av brandväggsregler med hjälp av -j logdrop .

Brandväggsregler

- Ta reda på vad datorn har för IP−adress:
  - ME=‘/sbin/ifconfig eth0 |sed −n ’/inet/s/^[ ]*inet addr:\([0−9.]*\).*/\1/p’‘
- Sätt upp en regel som tillåter datorn att prata med sig själv.
  - /sbin/iptables −A INPUT −−in−interface lo −j ACCEPT
- Notera att brandväggsreglerna används i den ordning de står.

Brandväggsregler

- Sätt upp regler som spärrar ut viss trafik.
  - Spärra ut och logga netbus−trafik.
    - /sbin/iptables −A INPUT −p tcp −−destination−port 12345 −j logdrop
    - /sbin/iptables −A INPUT −p udp −−destination−port 12345 −j logdrop
  - Spärra ut näten 10.0.0.0/8, 172.16.0.0/12 och 192.168.0.0/16
    - /sbin/iptables −A INPUT −−source 10.0.0.0/8 −j DROP
    - /sbin/iptables −A INPUT −−source 172.16.0.0/12 −j DROP
    - /sbin/iptables −A INPUT −−source 192.168.0.0/16 −j DROP

Brandväggsregler

- Släpp in viss ICMP−trafik. 0 och 8 används av ping, 3 är Destination Unreachable, 11 är Time Exceeded och används bland annat av traceroute.
  - # Släpp in Echo−Reply
  - /sbin/iptables −A INPUT −p icmp −−icmp−type 0 −j ACCEPT
  - # Släpp in Echo Request
  - /sbin/iptables −A INPUT −p icmp −−icmp−type 8 −j ACCEPT
  - # Släpp in Destination Unreachable
  - /sbin/iptables −A INPUT −p icmp −−icmp−type 3 −j ACCEPT
  - # Släpp in Time Exceeded
  - /sbin/iptables −A INPUT −p icmp −−icmp−type 11 −j ACCEPT

Brandväggsregler

- Nästa steg är att sätta upp brandväggsregler in till de egna servertjänsterna. Reglerna laddar modulen state och accepterar endast nya föbindelser.
  - Öppna upp till ssh, port 22.
    - /sbin/iptables -A INPUT -p tcp --destination−port 22 -j ACCEPT
  - Öppna upp till mailservern, smtp port 25.
    - /sbin/iptables -A INPUT -p tcp --destination−port 25 -j ACCEPT
  - Öppna upp till webservern, port 80.
    - /sbin/iptables -A INPUT -m state --state NEW -p tcp --syn --dport 80 -j ACCEPT
    - /sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -p tcp --dport 80 -j ACCEPT

Brandväggsregler

- För den egna trafiken, den som etableras utåt, måste svarstrafiken släppas in.
- Sätt upp en regel för svarstrafiken.
  - /sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
- Om all övrig inkommande trafik inte bara ska kastas utan även loggas behövs en regel för det.
  - /sbin/iptables -A INPUT -j logdrop

Spara brandväggsreglerna

- Ett sätt att se till att brandväggsreglerna alltid körs vid boot är att stoppa in dem i ett skalprogram och se till att skalprogrammet körs i samband med boot.
- I RedHat Linux (7.0 − 7.2) stäng av ipchains och slå på iptables.
  - chkconfig ipchains off
  - chkconfig iptables on

Spara brandväggsreglerna

- Vidare måste du i RedHat ändra i filen /etc/rc.d/init.d/iptables:
  - if /sbin/lsmod 2>/dev/null |grep -q ipchains ; then
  - # Don’t do both
  - exit 0
  - fi
- Efter fi lägg till följande:
  - if ["$KERNELMAJ" -eq 2 -a "$KERNELMIN" -eq 4]; then
  - if [! -f /proc/net/ip_tables_names]; then
  - modprobe iptables >/dev/null 2>&1 || exit 0
  - fi
  - fi

Spara brandväggsregler

- Under RedHat se till att köra brandväggsreglerna för hand eller från ett skalprogram.
- Spara därefter brandväggsreglerna i /etc/sysconfig/iptables med:
  - iptables-save > /etc/sysconfig/iptables

Maskerande brandvägg

- Om du har endast en publik IP−adress och vill ansluta fler än en dator kan en Linuxmaskin användas till maskerande brandvägg.
- Till detta behövs en dator med Linux och två nätverkskort.

Maskerande brandvägg

- Använd någon av de IP−nummerserier som är till för internt bruk för det interna nätet. Exempel, 192.168.22.0/24.
- Ge eth0 på brandväggen en IP−adress på ovanstående nät, tex. 192.168.22.1.
- Ställ in den adress som eth1 ska ha.
- Slå på routingen på brandväggen med:
  - echo 1 >/proc/sys/net/ipv4/ip_forward
- Stoppa in raden i t.ex. rc.local så att den körs vid boot.

Maskerande brandvägg

- Sätt upp standardregler
  - /sbin/iptables -P INPUT DROP
  - /sbin/iptables -P FORWARD DROP
  - /sbin/iptables -P OUTPUT ACCEPT
  - # Rensa bort gamla brandväggsregler
  - /sbin/iptables -F
  - /sbin/iptables -t nat -F
  - # Rensa bort gamla kedjor
  - /sbin/iptables -X

Maskerande brandvägg

- Om maskeringsstödet är kompilerat som modul ladda kärnmodulen iptable_nat och modulerna för övriga tjänster du använder.
- Spara yttre adressen i en variabel:
  - MEeth1=‘/sbin/ifconfig eth1 | sed −n ’/inet/s/^[ ]*inet addr:\([0−9.]*\).*/\1/p’‘
- Spara inre adressen i en variabel:
  - MEeth0=‘/sbin/ifconfig eth0 | sed −n ’/inet/s/^[ ]*inet addr:\([0−9.]*\).*/\1/p’‘

Maskerande brandvägg

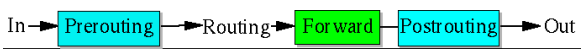
- Skapa kedjan logdrop.
  - /sbin/iptables -N logdrop
  - /sbin/iptables -A logdrop -j LOG
  - /sbin/iptables -A logdrop -j DROP
- Släpp ut all form av trafik från det interna nätverket:
  - /sbin/iptables -A FORWARD --in-interface eth0 -j ACCEPT
- Släpp in svarstrafik:
  - /sbin/iptables −A FORWARD --in-interface eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT

Maskerande brandvägg

- Maskera all utgående trafik genom att ändra avsändaradressen till brandväggens yttre adress.
  - /sbin/iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to $MEeth1
- Spärra och logga resten.
  - /sbin/iptables -A INPUT -j logdrop
  - /sbin/iptables -A FORWARD -j logdrop

Maskerande brandvägg

- Nu är brandväggsreglerna uppsatta och maskeringen för avsändaradresserna uppsatt.

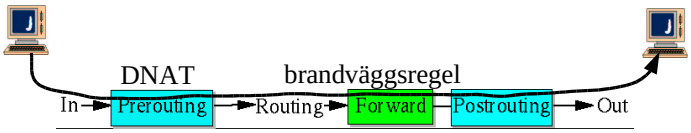


Maskerande brandvägg

- Inga datorer på det interna nätverket är nåbara utifrån.
- För att nå en servertjänst på en dator på det interna nätverket behövs en forwarding, DNAT, av trafiken.
- Forwarding ordnas med PREROUTING.
  - Skicka vidare all trafik till port 22 på brandväggens yttre interface in till 192.168.22.17 port 22.
    - /sbin/iptables -t nat -A PREROUTING -p tcp -d $MEeth1 --dport 22 -j DNAT --to 192.168.22.17:22

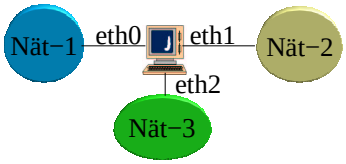
Maskerande brandvägg

- Mottagaradressen omvandlas i PREROUTINGEN.
- Till detta behövs även en regel i FORWARD−kedjan som släpper in trafiken.
  - /sbin/iptables -A FORWARD --in-interface eth1 -p tcp -d 192.168.22.17 --dport 22 -j ACCEPT



Exempel på regler för en brandvägg med tre interface

- # Sätt upp standardregel för FORWARD och kasta gamla regler
- iptables -P FORWARD DROP
- iptables -F
- # Sätt upp en regel som släpper in ssh−trafik från nät−1 till nät−2
- iptables -A FORWARD --in-interface eth0 --out-interface eth1 -m state --state NEW -p tcp --destination-port 22 -j ACCEPT
- # Sätt upp en regel som släpper in mail−trafik till 195.12.13.14 på nät2
- iptables -A FORWARD --out-interface eth1 -m state --state NEW -p tcp --destination-port 25 --destination 195.12.13.14 -j ACCEPT



Exempel på regler för en brandvägg med tre interface

- # Sätt upp en regel för svarstrafik från nät−2 bakom eth1
- /sbin/iptables -A FORWARD --in-interface eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT

Referenser och länkar

- Maximum Linux Security
  - Sams Publishing
  - ISBN: 0−672−31670−6
- http://www.lysator.liu.se/~kjell−e/tekla/linux
- http://www.cert.org/
- http://securityfocus.com/
- http://linuxsecurity.org/
- http://netfilter.samba.org/

Mailinglistor

- Följande mailinglistor är några av dem som finns på http://securityfocus.com
  - bugtraq
  - incidents
  - focus−linux