Studietips 3 -- Advanced Enterprise Linux Administration

Labbarna

Laboration 4, att använda och säkerhetskopiera Access Control Lists (ACL). En spännande och lärorik labb som omfattar många intressanta delar. Att sätta upp access listorna brukar inta vara något stort problem; det kan ju vara lite knepigt att komma på att modifiera **/etc/fstab**. Backupdelen kräver lite mer eftertanke, dels för att vi har ett schema att följa (cron...) men även för att man vill ha med ACL:erna. De flesta verkar ha insett att gnu-tar har en speciell switch för ta med ACL:er. Trots detta kan det ju kännas säkert att använda getfacl för att ytterligare öka möjligheterna att få saker att fungera efter en olycka.
Somliga har även nosat på den **frivilliga** labben om SELinux (**nummer 5**). Ni kommer ju att få chans att bekanta er mer med SELinux nästa år. Många låter helt enkelt bli denna besvärliga del av linux; felställda säkerhetskontext gör att saker kan sluta fungera utan ledtrådar i form av felmeddelanden, på en tung server med många tjänster kan detta leda till ett veritabelt träsk av problem, som ibland kan vara, i det närmaste, omöjligt att reda ut. På mer målinriktade maskiner med ett fåtal tjänster blir det naturligtvis mycket enklare. Å andra sidan är det alltid enklare att felsöka enkla system, att begränsa antalet tjänster kan alltid vara en bra början för de som vill ha ett säkert system, så SELinux kanske tvingar administratören till eftertanke och ordning.

Pluggandet

Kap 10, PAM - Pluggable Authentication Modules

Mycket användbar teknik, ni skall -på det här stadiet- känna till den och veta att PAM används av de flesta program som kräver autenticering av användare (inloggning alltså).
Ni skall även veta att det går att konfigurera olika parametrar om hur användaren får välja lösenord, när han får logga in och även saker som ”bäst före” datum på lösenord. En annan viktig aspekt är att PAM medger utbyte av användarnamn och lösenord till helt andra saker, allt från biometri (avläsning av fingeravtryck, näthinnor och DNA, för att nämna några saker). Men ni kan vänta till systemsäkerhetskursen nästa år med att fördjupa er i hur detta konfigureras.

Kap 11, Security Administration

Det är viktigt att ni förstår att enkelhet och ordning är två hörnpelare för systemsäkerhet. Den som lägger på alla paket han hittar och fipplar runt med systemet som om vore det en speldator, han skall inte ha någon anledning att förvåna sej den dagen servern blir crackad.
Ta bort tjänster som inte behövs, blockera konton som inte används; se över systemet så att rimliga lösenord används, bara små bokstäver, eller personnamn, könsord och populära gestalter från populärkulturen hör inte hemma som lösenord på ett säkert system. Det må vara att så väl Hitler, Voldemort, Dracula som Sauron, var och en på sitt sätt kan vara fasansväckande, men de skrämmer inga inkräktare. Använd **/etc/hosts.allow** och **/etc/hosts.deny**. **iptables** är naturligtvis lika praktiskt som det kan vara bökigt att använda, skaffa ett bra redskap att trimma **netfilter** om du inte kommer överens med kommandot **iptables**. Ta bort SUID och SGID behörigheten överallt där den inte är helt nödvändig.

Ladda gärna hem redskap för att crackers, den populära distributionen BackTrack (**http://www.backtrack-linux.org**) kan vara en bra startpunkt. När du kikat runt på vilka metoder ”kidsen" kör med begriper du bättre hur viktigt skydd kan vara.

Till specifika saker:

Behörighetslistor - ACL
Vid sidan av det gängse behörighetssystemet på UNIX/LINUX kan man lägga till ACL:er. Sådana finns inte till alla sorters filssystem och de fungerar inte om du inte slår på dem när du monterar filsystemet; /etc/fstab kan ju enkelt editeras...

setfacl -m u:voldemort:rw /ond/fil.txt	ger användaren voldemort läs och skriv på fil.txt
getfacl -r /ond> /bak.acl	backar behörighetslistorna i trädet /ond
setfacl --restore < /bak.acl	hämtar behörigheterna från backup
tar --acls -cf /ond.tar /ond	backar trädet /ond till filen /ond.tar

Private Group Scheme (UPG)
är populärt, men förleds inte att tro att det är det ända vettiga sättet att administrera en linuxkärra med hjälp av traditionella behörigheter (utan ACL).

SELinux
är en modul som ger kärnan möjlighet att ge varje process ett säkerhetskontext där det nogrant definieras vilka filer och resurser som får utnyttjas. Detta är naturligtvis mycket kraftfullt, men kan ofta upplevas som besvärligt och krångligt. Det är lätt att skapa ett system som varken fungerar eller ger vettiga loggar som förklarar varför.
Ni skall veta *ungefär* hur det fungerar, på säkerhetskursen nästa år får ni bekanta er närmare med koncepten.

Kapitel 12, Process Administration

Vid sidan av **at** och **batch** är det huvudsakliga redskapet för automation **crond** med kommandot **crontab**. På CentOS finns både anacron som framför allt hjälper de som inte kör sina datorer dygnet runt, så detta är inte så intressant för serverdrift; vixie cron som är Paul Vixies implementation av cron-systemet är däremot ett mycket viktigt verktyg som du bör bekanta dej med.

man crontab	berättar om kommandot crontab
man 5 crontab	berättar om syntaxen på en crontab-fil

Normalt kan du ofta strunta i de finare detaljerna i crontabbar om du bara vill köra saker regelbundet: gör ett vanligt shell-skript som du lägger i **/etc/cron.daily**; inga speciella krav på syntax, bara ett vanligt skript. **crond** kommer då att köra programmet dagligen; vill du i stället köra det varje timme väljer du **/var/cron.weekly** och så vidare.
Behöver du mer precis kontroll kan du antingen editera /etc/crontab eller skapa en egen crontab-fil som du lägger till med hjälp av kommandot crontab. *Det är en viktig skillnad på syntaxen mellan **/etc/crontab** och vilken crontab-fil som helst: den första kräver att du skriver **användarnamnet efter tidsangivelsen** så att crond vet vilken användare som skall användas för att köra varje kommando. I en vanlig crontab-fil så kör crond programmen som filens ägare.* Eventuell utdata från programmen i cron, skickas på epost till crontab-filens ägare; så använd rörledningar till **/dev/null** om du vill slippa att bli spammad av crond.

Process accounting kan vara intressant, men grotta inte ned er i detta. Däremot skall ni behärska kommandon som ps, top, kill, killall, nice och renice. Likaså bör ulimit finnas i arsenalen, så att du kan begränsa resursanvändningen på användar- och process-nivå.

Kapitel 13, Basic Networking och Kapitel 14, Advanced Networking

För den rena nätverkskompetensen har vi CISCO-blocket, med detta inte sagt att det kan vara bra att titta på det här avsnittet eftersom vi ju kommer att tala en mycket om nätverkstjänster i nästa kurs. Ntp kan dock vara en viktig del för att NFS och andra saker skall fungera väl. Det är dock några saker som är helt nödvändiga för er linuxdrift, först och främst konfigurationsfiler som:

/etc/services
lista över vanliga nätverkstjänster, protokoll och portnummer

/etc/resolv.conf
konfiguration av namnservrar och sökdomän (dns), kudzu kan bråka här

/etc/sysconfig/network-scripts
den katalog där du hittar grundläggande nätverksinställningar för ipadresser, nätmasker, routing och annat.

ifconfig
grundläggande kommando för att styra nätverksgränssnitten, addressering och liknande; resultatet tar omgående, men skall du ha permanenta inställningar som håller sej efter en omstart måste du använda filerna i **/etc/sysconfig/network-scripts**.

ifconfig eth0 10.10.4.42 netmask 255.255.255.0	ställer eth0 till 10.10.4.42/24
ifconfig eth0 10.10.4.42/24	ställer eth0 till 10.10.4.42/24 (precis som ovan)
ifconfig eth0:1 10.10.4.43/24 up	ställer och aktiverar en ytterligare ip med mask på eth0

ifup och **ifdown**
är två praktiska kommandon som aktiverar eller avaktiverar nätverksanslutningen

ifup eth0	startar trafik på eth0
ifdown eth0	stänger av tra

route
konfigurerar och visar routinginställningar; hur datorn hanterar paket till andra nätverk än det lokala.

route add default gw 10.10.4.1	ställer standardadress för att vidarebefordra paket till andra nät (default gateway) till 10.10.4.1
route del default	tar bort ovanstående
route -n	listar rutter
route add -net 10.10.4.0/24 gw 172.16.52.2	lägger till rutt för ett helt nät
route add -host 10.10.4.10 ppp0	lägger till rutt för specifik dator

arp
ARP står för Address Resolution Protocol, som används för att uppdatera information om hur paket skall skickas till olika destinationer. **arp** är ett kommando för att manuellt hantera rutt-tabellen.

arp -a	listar rutt-tabellen

arp -d 10.10.4.43	tar bort rutten till 10.10.4.3
arp -s 10.10.4.97 00:01:02:03:04:05	kopplar ipadressen 10.10.4.97 till en macadress.

ip
är en modern ersättare till de flesta av ovanstående kommandon. De flesta böcker och handledningar på nätet använder fortfarande de gamla varianterna; rent praktiskt är det ingen skillnad på vilken variant du väljer, men många av dina kollegor kan känna sej främmande till nymodigheter. Speciellt om de moderna varianterna inte ger några praktiska fördelar.

netstat och **lsof**
netstat visar information om nätverksanslutningar, uppkopplingar, rutt-tabeller, statistik, vilka program som lyssnar på vilken port och annat tekniskt om nätverket. **lsof** berättar vilka program som lyssnar på olika portar, vilka program som ansluter någonting på en port; saker som netstat också visar. Men **lsof** kan även ge upplysning om vilka filer ett program använder just nu, praktiskt om du har svårt att avmontera ett filssystem för att någon process använder någon fil där.

På ditt personliga system kan du naturligtvis använda program som exempelvis **NetworkManager** eller exempelvis **wicd** för att ställa grundparametrar på olika nätverksgränssnitt. Detta kan vara helt nödvändigt om du skall du drifta servrar för mobila tillämpningar, exempelvis som de system som SL använder i bussarna för stationsutrop och skyltar. Annars torde dessa verktyg mest höra till skrivbordet, där de ju kan vara mycket användbara.

Kapitel 15, X Window

Eftersom detta är en serverorienterad utbildning finns det ingen direkt anledning att ägna tid åt detta avsnitt, ur skolans perspektiv. Däremot kanske många känner intresse av att förstå hur X fungerar och då kan det ju vara trevligt att läsa lite här...

Kapitel 16, Log File Administration

Det är inget mystiskt med loggar, men ni skall veta var de finns. Hur ni konfigurerar syslogd (/etc/syslog.conf), likaså måste ni inse att syslog kan skicka loggar över nätet till någon central server; eller kanske administratorns skrivbord...
Ni bör också veta hur och varför loggarna skall roteras.
Glöm inte **dmesg**...

Kapitel 17, Monitoring and Troubleshooting

Övervakning och felsökning är viktigt. **top**, **free**, **swapon**, **vmstat, iostat, mpstat** är en kort lista över enkla, men viktiga kommandon. /proc/cpuinfo är en fil som berättar vad du har för processor.
Monitoreringsprogram som sar kan vara bra, men många kommer att kunna gå igenom en hel karriär utan att komma i närheten av dessa; men tung serverdrift och det kan vara din bästa vän...
strace är även det ett program som somliga aldrig kommer att behöva och som andra inte kan leva utan; oftast är det väl de mer programmeringsinriktade som behöver det.

Läs igenom och fundera över hur man felsöker, även här kan ordning och reda vara viktigt. Men även erfarenhet och instinkt (som man får genom erfarenhet); man blir aldrig gammal och klok om man inte varit ung och dum...
Boken tar ju upp räddningsmiljön på CentOS boot-skivor, fungerar helt OK i många fall, men de flesta brukar uppleva system som exempelvis följande:

Parted Magic
http://partedmagic.com/

Super Rescue CD
http://www.kernel.org/pub/dist/superrescue

Knoppix
http://www.knoppix.com/

som betydligt roligare. Ofta går det enkelt att klämma in sådana dist:ar på en minnepinne.

Lycka till,
Rolle.