Linux Säkerhet

Av

Glenn Larsson

(INFOSÄK-D, KY - Enköping)

—

(Originaldokumentet skapades 2005-Februari-17, korrigering och konvertering till PDF format har skett 2009-April-03)

____

(Glenn Larsson)

Innehållsförteckning

Förord

Detta dokument är en sammanställning av det INFOSÄK D klassen gick igenom på Linux kursen VT 2005. Dokumentet riktar sig till erfarna tekniker och avancerade användare som har ett intresse av att lära sig om säkerheten i Linux. Läraren på kursen var Tom Johansson.

I detta dokument så återfinns delar av det som togs upp på kursen, specifikt säkerhetsdelen av Linuxkursen (servermjukvara som t.ex Postfix och Apache utelämnas helt) samt en del extra material som av författaren ansågs matnyttigt för läsaren (t.ex Forensics, Intrusion Detection och PAM).

Enköping, 2005
Glenn Larsson

Bakgrund

Linux är ett modernt operativsystem som har ökat stort på server marknaden de senare åren. Det finns flera varianter av Linux och det är viktigt att känna till det samt att veta vad du som systemansvarig kan göra för att öka säkerheten.

Sammanfattning

Syftet med detta dokument var att sammanställa det vi gick igenom på Linux kursen. Då uppgiften var att skriva om säkerheten i Linux så har dokumentet begränsats till att enbart beskriva säkerheten i systemet.

Dokumentet är uppdelat i följande delar;

- **Hardening – Att säkerställa ett Linux system**

  Här beskrivs några steg som kan tas för att säkra upp systemet.

- **Loggning**

  Här beskrivs logfiler och SyslogD.

- **Intrusion Detection – Att upptäcka intrång**

  Denna del beskriver några metoder och mjukvaror som kan upptäcka intrång, t.ex IDS systemet "Snort".

- **Intrusion Prevention – Att förhindra intrång**

  Denna del beskriver förhindrande av intrång med aktiva medel, t.ex "IPTables" och "TCPWrappers".

- **Patchning**

  Beskriver uppdatering av både mjukvara och Kernel.

- **Auditering**

  Denna del tar upp hur du kan verifiera att ditt system verkligen är säkert, dvs Auditering av systemet.

- **Forensics - Att säkra & undersöka digitala spår efter intrång**

  Den avslutande delen tar upp "Forensics" dvs vad du kan göra för att säkerställa och undersöka elektroniska spår efter intrång.

Hardening – Att säkerställa ett Linuxsystem

Denna del tar upp hur du kan säkerställa din Linuxserver. Här följer nu en del förslag på enkla insatser du kan göra för att reducera att ditt system råkar ut för angrepp och driftstörningar uppstår som result av detta.

- *Root kontot ska ha ett komplext lösenord.*

  Naturligtvis ska det ta lång tid att knäcka lösenordet på Root kontot. Ett starkt lösenord med tecken uppsättningen [**A-Z**] + [**a-z**] + [**0-9**], icke alfanumeriska tecken (!"$&Å{) är också önskvärda.

  Även om det är hyffsat svårt att komma över **/etc/passwd** och **/etc/shadow** filerna (vilka innehåller konton och lösenord) så är svårigheten att komma över dessa filer ingenting som du ska förlita dig på - säkerhet är en kedja som brister av den svagaste länken.

- Sätt upp lösenords policy

  Konfigurera din Linux server så att inga lösenord får vara äldre än 60 dagar, längd på lösenordet, antal inloggnings försök m.m. Detta gör du i filen

  /etc/login.defs

- *Installera PAM modulerna för starkare autentikering*

  Pluggable Authentication Modules (PAM) är en mjukvara för linux som förstärker autentikeringen och samtidigt ger dig större kontroll över detta, t.ex vad som ska hända om något oförutsätt händer.

  Vissa Linux distributioner kommer redan med PAM installerat (t.ex Suse Linux). Använd dig av MD5 algoritmen och stäng av alla andra autentikerings sätt (Speciellt NO PASSWORD). Du konfigurerar detta i filerna:

  /etc/security/pam_pwcheck.conf
  /etc/security/pam_unix2.conf

- *Installera TLS/SSL (OpenSSL/ModSSL) för tjänster som HTTPD (t.ex Apache).*

  Om du har tjänster som en webserver installerad, överväg att installera stöd för TLS (SSL3) i fall att känslig information finns på din server. Du kan ladda ner ett komplett TLS paket (OpenSSL och ModSSL) på dessa adresser:

  http://www.openssl.org/

  http://www.modssl.org/

  *Notera: En installationshandledning för OpenSSL och ModSSL för Apache kan återfinnas på http://www.securityfocus.com/ , sök efter **"Apache 2 with SSL/TLS: Step-by-Step"***

- *Stäng av onödiga tjänster i InetD.*

  Om någonting inte är där så kan det inte göra skada. Ta därför bort onödiga tjänster ifrån ditt system som du inte använder.

  Du konfigurerar *INETD* i filen **/etc/Inetd.conf**
  Glöm inte bort att starta om INETD (*) för att dina ändringar ska få effekt.

  (* **killall –HUP inetd**)

- *Byt ut tjänster som kommunicerar i klartext, t.ex TelnetD & FTPD.*

  Då det är enkelt att angripa och avlyssna vilken dator som helst på internet så bör du byta ut tjänsterna på din server emot tjänster som inte pratar klartext utan kommunicerar krypterat, t.ex byts ut *TelnetD* emot *SSHD*.

  Notera: Detta gäller främst på äldre Linux installationer. Nyare Linux distributioner har oftast redan säkra tjänster som SSHD installerat och klartext tjänsterna är blockerade, men finns kvar för bakåtkompabilitet och kan vara aktiverade av bekvämlighet.

- *Root ska ej kunna logga in utifrån.*

  Ett sätt att enkelt säkerställa systemet är att inte tillåta root att logga in ifrån någon annat ställe än vid den fysiska maskinen där kontot finns. Detta konfigureras i filen

  /etc/security/access.conf

  (Naturligtvis kan dom med rättigheter alltid ändra allt i systemet och någon tekniker kan vilja vara bekväm och ta bort dessa spärrar. Därför är det viktigt att klargöra varför systemet är konfigurerat på på det sättet för administrativ personal då detta inte alltid är uppenbart.)

- *Tillåt inte administratörer att skjuta sig själva i foten.*

  I Windows världen används CTRL + ALT + DELETE för att logga in, i Linux är detta ett kommando som stänger ner/startar om systemet.

  Du kan enkelt förhindra att någon administratör av misstag sänker din produktionsserver igenom att ändra i filen: **/etc/inittab**

  Där letar du upp och ändrar följande rad:

  ca::ctraaltdel:**shutdown –t 5 -now**

  ..till exempelvis..

  ca::ctraaltdel:**echo "Ctrl-Alt-Delete is disabled by administrator"**

- *Ta bort onödiga saker ur Linux Kernel.*

VARNING: Här har du en chans att skjuta dig själv ordentligt i foten. Om du inte vet vad du håller på med så hoppa över detta steg eller låt en erfaren konsult sköta detta.

Åter igen, reducera riskerna - ta bort saker som inte behöver vara där, exempel: IPv6 implementationen(*) i kernel versionerna **2.4.20** and **2.6.4** visade sig vara sårbart emot en Denial of Service-attack som kunde få ditt system att krasha.

(* **Http://www.packetstormsecurity.com/0502-advisories/kernelOverflow.txt**)

Om du har Linux källkoden installerad så kan du bygga om din Kernel igenom att göra följande:

cd /usr/src/linux/
make menuconfig

När du är klar skapar du din nya kernel med kommandot:

make bzImage

Du kan boota ifrån flera olika Kernel filer. Om du kör *lilo* så konfigureras detta i filen **/etc/lilo.conf**, när du är klar så kör du kommandot **lilo** för att ändringarna ska sparas ner.

- *Kör inte tjänster som root, chroot'a dom tjänster som måste köras.*

Chroota – d.v.s. begränsa dina tjänsters sårbarhet, detta minskar rejält vad en angripare kan tänkas göra när denne väl är inne i systemet.

En beskrivning på hur du kan chroot'a tjänster återfinns på följande adress:

http://www.linuxfocus.org/English/January2002/article225.shtml

- *Ta bort informationsläckage*

I princip så står ditt system som standard och berättar för angriparen hur systemet ska angripas. Stoppa detta igenom att ta bort login och service banners ifrån ditt system.

Exempelvis så berättar Filerna **/etc/issue** & **/etc/issue.net** vilken Linux kernel du kör, Apache HTTPD servern berättar gärna för hela världen vilken version den är, online dokumentation och standard *cgi-scripts* i applikationens kataloger kan också avslöja vilken version det är som finns installerad såväl som systemets konfiguration.

Om du har tillgång till en applikations sourcekod så kan du även editera bort service banners ifrån nätverkstjänsterna. Här har vi ytterligare ett ställe där du bör veta vad du håller på med. Be någon annan sköta detta om du är osäker.

Loggning

Som standard så loggar dom vanligaste tjänsterna till fileri en katalog. Beroende på vilken Linux distribution du har installerad så kan dessa filer återfinnas i antingen **/var/log** eller i **/var/adm** katalogen eller på något annat ställe beroende på vilken Linux distribution du använder dig av.

Det är 3 filer du bör ha koll på som minimum:

- messages
- syslog
- secure

Dessa filer innehåller felmedelanden, inloggningar, transaktioner –allt som systemet är konfigurerat för att logga. Här kan du hitta intrångsförsök och felkonfigurerade tjänster som kan utgöra en säkerhets risk i systemet.

SyslogD är en tjänst som lyssnar på port UDP/514. Den kan konfigureras att logga ifrån en hel uppsjö av tjänster/program och även ifrån andra system. Nyligen nämndes *syslog* filen - det är SyslogD tjänsten som loggar till den filen.

Intrusion Detection – Att upptäcka intrång

Att upptäcka intrång i ett system kan vara svårt, Även om systemet loggar händelser så är ofta den informationen som kan sammanställas ur systemet ganska knapphändig. Den bästa lösningen idag är att installera att Intrusion Detection System (IDS) av något slag. Det finns en del kategorier; Fil IDS, Nätverk IDS och Kernel modul.

- *Tripwire*

  Tripwire är ett verktyg som scannar av filer och tittar på information som kan avslöja om en fil har blivit ändrad eller inte. Tripwire kan du ladda hem ifrån:

  http://www.tripwire.org/

- *Snort - IDS system för Linux*

  Snort är ett NIDS (Nätverks IDS) som läser av trafik som går in/ut ur nätverket. Detta hanteras enligt en lista med regler som påminner om brandväggsregler. Snort är open source och går att ladda ner ifrån:

  http://www.snort.org/

  LibPCap krävs för att Snort ska fungera och kan laddas ner ifrån

  http://www.tcpdump.org/

- *LIDS - Linus Intrusion Detection System*

  LIDS är en Kernel modul för Linux. Lids rapporterar systemhändelser, portscan försök och implementerar även Accesskontroller i systemet. För närvarande finns stöd för Kernel version 2.4.28, stöd för Kernel 2.6.10 är vid detta tillfället (2005-Feb-09) under utveckling)

  LIDS kan laddas hem ifrån:

  http://www.lids.org/

Dessa olika IDS system kompletterar varandra och informationen som dessa program samlar ska koordineras för att öka spårbarheten vid en incident.

Intrusion Prevention – Att förhindra intrång

Detta kan ske på olika sätt, ett sätt är att använda dig av accesskontroll (TCPWrappers) eller att använda dig av en brandvägg

- *Accesskontrol med TCPWrappers*

  Du lägger in vilka tjänster och hosts som du vill neka i filen **/etc/hosts.deny** och det motsvarande i filen **/etc/hosts.allow**.

  Ett problemet med TCPWrappers är att det fungerar endast för tjänster som är körs av TCPD.

- *Iptables - Brandvägg för Linux*

  IPTables är ett paketfilter (Brandvägg) som kan konfigureras att tillåta eller neka alla tjänster i ett system, inte bara dom som körs under TCPD. Du kan skapa en brandväggs funktion i din dator i scriptet

  /etc/rc.d/rc.firewall

  Du bör även skapa en del scripts för att blockera/öppna individuella tjänster samt allt om för att snabbt kunna låsa ditt system om ditt system blir angripet.

  För att se vilka portar du kanske bör blokeras skriver du:

  netstat –ant | grep “LISTENING”

  Begränsa åtkomsten till de systemen/näten du använder dig av, det finns ingen orsak att tillåta alla i hela världen ha åtkomst till ditt system och ej heller att låta alla i ditt nätverk ha åtkomst till alla tjänster.

  Om du har en äldre IPTables installerad, eller har ett system som inte levereras med IPTables så kan du ladda ner senaste versionen av IPTables ifrån

  http://www.netfilter.org/

Patchning

Det är viktigt att du håller ditt system patchat, detta gäller naturligtvis för alla system och inte abra Linux. Patchning gör att du slipper du otrevliga överaskningar som t.ex intrång, driftstopp eller informationsläckage.

- *Uppdatera din kernel.*

  Du kan ladda hem Sourcekod/Färdiga Kernel filer klara att användas ifrån:

  > **http://www.kernel.org/**

  Se **Hardening** delen hur du konfigurerar din kernel och reducerar risker.

- *Uppdatera mjukvaran i ditt system.*

  Den mjukvaran du kör ska hållas uppdaterad. Människor är inte perfekta och ibland smyger det in en bugg här och där. Därför bör du uppdatera mjukvaran regelbundet för att bli av med buggar och säkerhetsproblem.

Auditering

Säkerhet är bra, men att *auditera* att säkerheten verkligen är håller (t.ex att göra en säkerhets revision) måttet är guld värt då felkonfigureringar kan ske. Många säkerhetsprodukter är dessutom bristfälliga och kan variera kraftigt i funktionalitet.

- *Reducera "false positives" hos din Brandvägg/ditt IDS*

  Att logga händelser är bra, fast om loggarna skriker "Vargen kommer!" var femte minut kanske det helt enkelt inte är bra, du bör konfigurera ditt IDS system så att det enbart varnar när det verkligen behövs. Ta därför bort regler som inte gäller - det kostar processorkraft att leta/blockera saker som du inte behöver ha med.

- *Scanna dig själv*

  Det bästa sättet att se till att allt är att i sin ordning är att scanna sig själv med en säkerhetsscanner. Det finns en uppsjö av verktyg, många är dessutom gratis. Ett sådant verktyg är Nessus som du kan ladda hem ifrån:

  http://www.nessus.org/

  Det finns även en säkerhets variant av Linux (**Trinux**) som kan användas ifrån en annan dator för att scanna igenom ditt liux system efter sårbarheter

  http://www.trinux.org/

- *Ethereal*

  Ethereal är en nätverkssniffer som kan analysera nätverkstrafik och t.ex redan inspelad trafik (t.ex TCPDump), det har väldigt bra funktioner som t.ex "*Follow TCP Stream*" vilket låter dig se hela sessioner på nätet och kan även avslöja om dina tjänster pratar i klartext (okrypterat) eller är felkonfigurerade.

  http://www.ethereal.com/

  För att få Ethereal att fungera så måste du även installera *LibPCap* som du kan ta hem ifrån:

  http://www.tcpdump.org/

- *lsof*

  Lsof är ett kommando som listar Portar och deras relaterade Process Ids. Detta är ett bra sätt att hitta bakdörrar och onödiga tjänster som kan utgöra en säkerhetsrisk och du önskar att avinstallera.

- *NMap*

  NMap är en av dom bästa portscanners och klarar av mycket som kan hjälpa dig se om brandväggen verkligen gör sitt jobb. Den kan även identifiera vilket operativsystem som körs och vilken tjänst som verkligen körs på porten. Du kan ladda hem NMap ifrån:

  http://www.insecure.org/

  NMap kräver *LibPCap* som kan tankas hem ifrån:

  http://www.tcpdump.org/

- Sök efter felaktiga rättigheter

  De flesta Linux systemen idag är relativt säkra efter en grundinstallation när det gäller filsystemen. Å andra sidan har kataloger och filer en tendens att ändras. Du kan hitta felaktiga rättigheter med följande kommandon:

  find / -perm 0777 ! -type f

  find / -perm 0777 ! -type d

  Förklaring till kommandoswitcharna

  -type f = listar filer som har rättigheterna 0777
  -type d = listar kataloger som har rättigheterna 0777

Användning

Denna del av dokumentet tar upp saker om handhavandet av Linux.

- *Sudo/SU*

  Logga inte in som root som standard, Använd dig av Sudo och SU kommandona om du vill göra någonting som root.

- *Säkerställ att någon läser loggar*

  Loggarna är endast till nytta om någon läser dom, t.ex. en säkerhetsansvarig eller en tjänst som använder dom för att konfigurera en annan tjänst (t.ex en brandvägg)

- *Om att lägga till users/groups*

  När du lägger till användare (**adduser**) och grupper (**groupadd**) så kan det vara bra att du anger kontaktinformation till användaren så att du kan kontakta denne vid behov (t.ex vid misstanke om intrång)

- *Om sätta rättigheter*

  När du sätter rättigheter (**chmod**) och tillhörighet (**chown**) på filer/katalogen så bör du fråga dig själv om övriga och gruppmedlemmar verkligen behöver några rättigheter/åtkomst alls på det objektet? Var restriktiv. Rättigheterna finns dokumenterade i manual dokumenten för **chmod** och **chown**.

- *htpasswd*

  Htpasswd är ett kommando för att skapa *CRYPT* genererade lösenord för autentikering i server applikationer som *VM-POP3D* och *Apache HTTPD*. Det kan även användas för att skapa lösenord i *MD5*/*SHA-1* format.

- *md5sum*

  Md5sum tillåter dig att skapa/validera MD5 signaturer på filer, oftast används detta kommando att verifiera/validera innehållet i en fil du tankat hem ifrån internet. Det gör du så enkelt som

  md5sum filnamn

  Vill du skapa en signatur på en fil du ska göra tillgänglig på internet:

  md5sum filnamn >filnamn.signatur

Forensics – Att säkra & undersöka digitala spår efter intrång

När en incident uppstår (intrång etc) så kan det vara bra att veta hur du hanterar systemet, fil systemen och loggfiler. Normalt sätt så bör detta lämnas till ett proffs som kan sin sak, så är du osäker så ska du aldrig försöka dig på detta då dina handlingar kan förstöra bevis.

- *Hantera loggar med kommandon:*

  Loggfiler kan vara stora, då är det bra att veta hur du hittar information i dessa. Komplett kommandoreferens över ett kan du få om du skriver **man kommando** där kommando är ett av dom följande listade kommandona. ("man" är kort för maunal under Linux)

  diff – visar skillnader emellan textfiler

  head – visar textfiler ifrån början

  tail – visar textfiler ifrån slutet

  grep – hittar innehåll i textfiler (som FIND under MSDos)

  strings – Söker efter strängar i text och binära filer

  sort – Sorterar innehållet i textfiler

- *Att använda dd för att spara ner bevis ifrån ett filsystem*

  Dd är ett kopierings kommando du kan använda dig av vid incidenter för att spara ner bevis.

  Innan du går vidare så måste du först se till att inga tjänster är igång som ändrar data på den enheten som du skapar en image ifrån. Det gör du lättast igenom att boota upp en installation/recovery CD/Diskett och mountar enheterna.

  Här är ett exempel på hur du sparar ner en partition (HDA1) till under katalogen **/stuff**. **/stuff** måste naturligtvis vara på en annan enhet än den du kopierar data ifrån.

  dd if=/dev/hda1 of=/stuff/hda1_ext2.dd

  (Notera att i namnet så anger vi "**ext2**" dvs vilket filsystem som används) Direkt efter detta skapar du en signatur på partitionsfilen med *md5sum*:

  md5sum /stuff/ hda1_ext2.dd > hda1_ext2.dd.md5

  Du kan nu analysera systemet i lugn och ro på ett annat system med verktyget *Sleuthkit* som beskrivs på nästa sida.

  Det går även att montera dd filen som ett filsystem i fall att du vill undersöka filsystemet manuellt med dom verktygen som följer med i standard Linux distributionerna. Var noga med växlarna **–r** och **–o noexec** då du kan förstöra data/få in fientlig kod i ditt system annars:

  Mount –r –t ext2 –o noexec, loop /path/hda1_ext2.dd /hda1

- *Sleuthkit*

  Sleuthkit är ett "Forensics kit" för Linux som har ett antal kommandon som underlättar vid undersökning av kompromitterade system.

Här följer en lista med dom filerna som följer med i Sleuthkit 1.73:

fsstat – visar detaljer om filsystemet
dcat – visar detaljer om delar av det använda filsystemet
dls – Visar info om icke allokerade/borttagna filer
ils & **istat** – visar strukturell information om (JFS)filsystem
icat – visar innehåll ur allokeringsenheterna
ifind – visar relationer emellan filnamen och allokerings enheterna
fls – visar filer/kataloger, även borttagna
ffind – visar relationer emellan allokeringsenheterna och filnamnen
mactime – hjälper till att skapa en timeline för händelser
hfind – skapar en sökbar databas med hash(md5/sha-1) signaturer
sorter – kategoriserar filer, t.ex fungerande ifrån korrupta

Sleuthkit kan du ladda hem ifrån:

http://www.sleuthkit.org/

Där finns det också dokumentation om hur mjukvaran fungerar. Det mest välciterade källan om Computer Forensics är Project Honeynet som kan nås på:

http://project.honeynet.org/

- *Rootkit hunter*

Rootkits är program som har parasiterat sig in i operativsystemet, en sorts extrem parasiterande bakdörr som är svår att få bort då har grävt ner sig så långt ner i systemet så den kan gömma sig för kommandon som **ps**, **ls**, **lsof** och andra kommandon (*då dom kommandona troligtvis också har blivit infekterade!*)

Rootkit hunter scannar igenom filsystemet och jämför signaturer, rättigheter, Linux Kernel Moduler och välkända filer ifrån rootkits/bakdörrar.

RKHunter kan laddas hem ifrån:

http://www.rootkit.nl/projects/rootkit_hunter.html

Slutsats

Linux är ett komplext system som har en hög inlärningströskel då dom flesta har svårt att skriva kommandon och blir lätt bortskrämda ifrån alla kommandon. Det är viktigt att tänka på alla steg i säkerheten och inte bara att installera en brandvägg. Vilken nytta gör en brandvägg om den släpper igenom bakdörrar som kommunicerar på TCP-port 80 då du för att du släpper igenom all traffik in till din Apache server som också kommunicerar på TCP-port 80?

Det är därför viktigt att du säkrar upp ditt system för att minimera riskern att något ska gå fel. 100% säkerhet är en myt. Det är viktigt att sådant som uppstår loggas, att loggarna läses och att något sker när någonting händer. Att du kan se när ett intrång sker och vad som har hänt är också viktigt och sedan förhindra att intrånget sker igen.

Du ska även patcha ditt system regelbundet så att buggar försvinner ur mjukvaran. Auditera ditt system då och då så att du vet att det är säkert. Lär dig använda systemet på ett säkert sätt, om du är osäker - sätt dig på skolbänken eller köp en bok. Forensics; hur du säkerställer bevis vid en incident är viktigt om du är en vanlig måltavla för intrång.

Rekommendationer

Ta säkerheten i Linux på allvar. Som ansvarig för ett system så bör du kunna säkra upp systemet till en tillräcklig nivå för att dom största riskerna minimeras. Nisses blomhandel kanske inte låter som en direkt måltavla men om Nisses server används för att angripa andra system så blir situationen helt plötsligt annorlunda.

Om du vill lära dig mera om säkerheten i Linux så har Securityfocus ett stort onlinebibliotek om detta och mycket annat, du når Securityfocus på:

http://www.securityfcus.com/

Om du vill tanka hem verktyg för att testa säkerheten i Linux, eller om du är ute efter en ny funktion för ditt system så kan du hitta verktyg för det på adressen:

http://www.packetstormsecurity.com/

Referenser

Dokument:

- Antekningar ifrån kursen
- CHRoot av tjänster
  http://www.linuxfocus.org/English/January2002/article225.shtml
- Website med (bland annat) ett stort online bibliotek om säkerheten i Linux:
  http://www.securityfocus.com/
- Website med verktyg för att testa säkerhet:
  http://www.packetstormsecurity.com/

Mjukvara:

- Slackware 8.0 - Operativsystemet som användes
- OpenSSL / ModSSL - Krypteringslösning för t.ex *Apache*
- L.I.D.S. - Kernel IDS
- Snort - Nätverks IDS
- Tripwire - Fil integritets IDS
- Ethereal - Sniffer gränssnitt för *LibPCap*
- TCPWrappers - Program för accesskontrol (TCPD-tjänster)
- IPTables - Brandvägg för Linux
- NMap - Avancerad Portscanner för Linux
- LibPCap - Promisc-drivrutin för Linux
- Nessus - Säkerhets scanner för Auditering
- Trinux - Linuxvariant som används för att Auditering.
- lsof - Program för att hitta Tjänster/Bakdörrar
- netstat - Mjukvara som visar status på TCP/IP tjänster.
- dd - Kommando som kan användas för att spara ner “snapshots” av partitioner
- Md5sum - Kommando för validering av data
- Sleuthkit - Forensics kit för partitioner
- Rootkit hunter - Program för att hitta Rootkits i Linux