

Knoppix STD 0.1 (Syphilis)

Zakazana dystrybucja...



stępną z poziomu menu i można je od razu wypróbować.

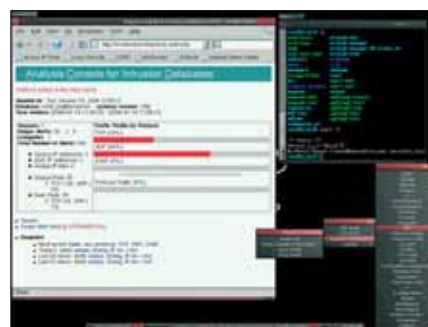
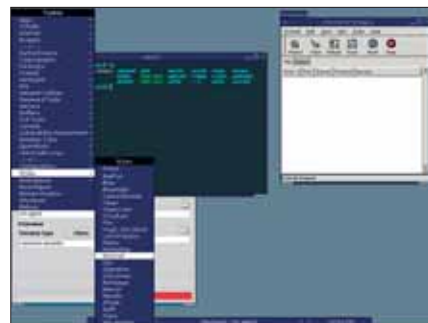
Linux-STD to znakomite narzędzie edukacyjne oraz diagnostyczne. Trzeba jednak pamiętać, że w nieodpowiednich rękach to narzędzie może służyć do niecnych celów takich jak włamanie na serwery czy do sieci firmowych. Nie na darmo wydanie 0.1 nosi wymowną nazwę Syphilis...

Więcej informacji na temat dystrybucji i zawartych w niej narzędzi można znaleźć pod adresem <http://www.knoppix-std.org>.

Dodatkowo...

Na CD-ROM znajdziecie także programy opisane w artykułach zamieszczonych w tym numerze Linux Magazine (między innymi serwer Asterisk i klientów VoIP dla Linuksa). Dodatkowo przygotowaliśmy specjalną atrakcję – na płycie znajduje się pełne archiwum wszystkich artykułów opublikowanych w Linux Magazine 1/2004 (lutym). Artykuły publikujemy w łatwym do przeglądania i wydruku formacie PDF.

Oprócz ustawień na dysku można przecho-



Knoppix-STD to specjalna wersja najpopularniejszej dystrybucji Live-CD (uruchamianej bezpośrednio z płyty CD-ROM). Została ona przygotowana tak, aby zawierała jak najwięcej narzędzi związanych z bezpieczeństwem. Rzeczywiście, ilość i jakość narzędzi robi wrażenie, na płycie znajdziemy narzędzia związane z szyfrowaniem plików, audytem zabezpieczeń, a skończywszy na skanerach antywirusowych i snifferach dla sieci bezprzewodowych. Knoppix-STD jest uważany za jedno z najlepszych narzędzi tego typu.

Knoppix-STD to nowa dystrybucja, która (tak jak Knoppix) znakomicie radzi sobie z wykrywaniem sprzętu oferując od razu możliwość pracy w trybie graficznym. Interfejs użytkownika zapewnia szybki menedżer okien – Fluxbox, wszystkie aplikacje są łatwo do-

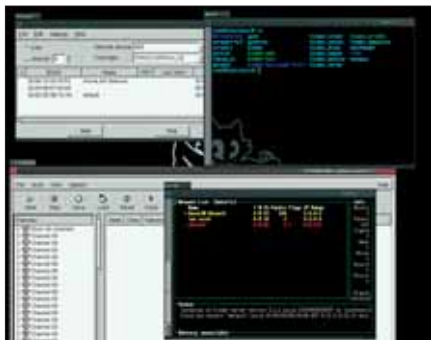
Mój dom jest wszędzie...

Przygotowanie i korzystanie z szyfrowanego katalogu domowego zapisywanego na zewnętrznym nośniku jest w Knoppix-STD łatwe (tak jak i w „normalnym” Knoppixie). Pozwala to na bezpieczne przechowywanie swoich preferencji i ustawień, mimo braku instalacji na twardym dysku. Knoppix oferuje możliwość zaszyfrowania katalogu domowego algorytmem AES o długości klucza 256 bitów.

Konfiguracja

Podłącz dysk USB do komputera ale nie

montuj go ręcznie. Uruchom narzędzie konfiguracyjne z menu „K -> Knoppix -> Configure -> Create a persistent KNOPPIX Home directory”. Wybierz partycję docelową dla katalogu domowego, dyski USB są zazwyczaj „widoczne” jako urządzenie `/dev/sda1`. Jeśli nie chcesz na tym etapie określać z góry, która partycja ma być używana do zapisu katalogu domowego, wybierz opcję „No”. Zdefiniuj rozmiar katalogu domowego – domyślna wartość 30 MB może być dla niektórych użytkowników zbyt mała.



kończyć operację. Katalog domowy jaki ma być używany po starcie systemu można określić z poziomu menu startowego systemu np.:

```
boot: knoppix home=/dev/sda1
```

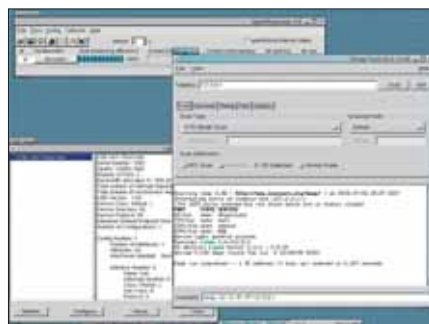
jeśli znasz nazwę partycji lub:

```
boot: knoppix home=scan
```

jeśli system ma samodzielnie próbować odnaleźć dostępne katalogi domowe. ■

wywać po prostu potrzebne pliki poza katalogiem domowym, do których będziemy mieli dostęp bez potrzeby podawania hasła. Katalog domowy (w postaci zaszyfrowanej) będzie widoczny jako plik *knoppix.img* i będzie montowany razem ze startem systemu.

Określ następnie czy chcesz szyfrować plik *knoppix.img*. Do szyfrowania używany jest algorytm AES wykorzystujący klucz 256-bitowy. System wymaga do zamontowania pliku wprowadzenia hasła, które ma co najmniej 20 znaków. Zdefiniuj hasło i pozwól systemowi za-



Instalacja na twardym dysku

Knoppix-STD można zainstalować na twardym dysku postępując zgodnie z następującą procedurą (niestety nie istnieje graficzne narzędzie instalacyjne, dlatego nie zalecamy tej operacji początkującym):

- 1) Uruchom komputer z płyty z Knoppix-STD
- 2) Utwórz pustą partycję ext2 i zamontuj ją np. w katalogu `/mnt/knoppix`
- 3) Skopiuj zawartość dystrybucji na dysk poleceniem `cp -a /KNOPPIX/* /mnt/knoppix/`
- 4) Skonfiguruj odpowiednio pliki `/mnt/knoppix/etc/fstab` i `/mnt/knoppix/etc/lilo.conf` dla nowego systemu i wykonaj polecenie `lilo`
- 5) Wykonaj polecenie `mkdir /mnt/knoppix/home/knoppix` oraz `chown knoppix.knoppix /mnt/knoppix/home/knoppix`
- 6) Uruchom ponownie system.

Prosimy pamiętać, że Knoppix-STD nie ma zdefiniowanego hasła dla użytkownika root.

Lista wybranych narzędzi zawartych w dystrybucji Knoppix STD 0.1 (wraz z nazwą katalogu w którym się znajdują):

Kategoria	Lokalizacja	Lista
Uwierzytelnianie	<code>/usr/bin/auth/</code>	freeradius 0.9.3: GPL RADIUS server
Szyfrowanie	<code>/usr/bin/crypto/</code>	acfe: narzędzie do analizy kryptograficznej; gpg: GNU Privacy Guard; mp3stego: steganografia dla MP3; openssl; stegbreak: szukanie danych w plikach JPG; stegdetect: wykrywanie steganografii; sslwrap, stunnel: narzędzia dla SSL; super-freeSWAN: implementacja protokołu IPSEC
Narzędzia do zabezpieczania dowodów	<code>/usr/bin/forensics/</code>	sleuthkit: narzędzie do zabezpieczania śladów włamania; biew: przeglądarka plików binarnych; coreography: analiza plików core; feris: śledzenie, dekompilacja i reverse engineering; galleta: analiza cookies z MS IE; hdb: dekompiletor dla Java; memfetch: wymuszanie zrzutu pamięci; pasco: analiza plików index.dat z MS IE; readdbx: konwersja skrzynek MS Outlook Express (.dbx) do formatu mbox
Zapory ogniowe (firewall-e)	<code>/usr/bin/fw/</code>	blockall: skrypt blokujący cały przychodzący ruch TCP (oprócz adresu localhost); firestarter: zaporę ogniową z graficznym GUI, firewall, floppyfw (tworzenie firewalla na dyskietce), fwlogwatch, gtk-iptables, shorewall
Przynęty (honeypots)	<code>/usr/bin/honeypot/</code>	honeyd, labrea, thp
IDS (Intrusion Detection Systems) – systemy wykrywania włamań	<code>/usr/bin/ids/</code>	dsnort 2.1.0, bro, prelude (systemy IDS), WIDZ – IDS dla WiFi
Narzędzia sieciowe	<code>/usr/bin/net-utils/</code>	LinNeighborhood (klient SMB); argus: audyt sieci; arpwatc; cheops: monitorowanie sieci przy pomocy SNMP; etherape, iperf, iptraf: monitoruj sieci; mrtg, ntop: sieciowa odmiana polecenia „top”
Narzędzia do łamania haseł	<code>/usr/bin/pwd-tools/</code>	john 1.6.34 (John the Ripper – klasyczny łamacz haseł), allwords2 (słownik angielski od CERIAS o objętości 27MB), chntpw (resetowanie haseł na maszynach z Windows), cmospwd (odnajdywanie hasła do BIOS), djohn (rozproszona wersja John the Ripper), pw19x (łamanie haseł Win9x)
Serwery	<code>/usr/bin/servers</code>	apache, ircd-hybrid, samba, smail, sshd, vnc, net-snmp, tftpd, xinetd
Sniffery	<code>/usr/bin/sniff/</code>	driftnet (sniffer szukający obrazków), dsniiff (sniffer haseł przesyłanych otwartym tekstem), ethereal (sniffer dla Ethernetu), ettercap (sniffer dla sieci przelączanych), mailsnarf (sniffer ruchu SMTP/POP), tcpdump (klasyczny sniffer sieciowy), urlsnarf (sniffer adresów URL)
Narzędzia dla TCP	<code>/usr/bin/tcp-tools/</code>	arpftech (pobieranie adresu MAC), arpspoof (spoofing ARP), despoof (wykrywanie pakietów typu spoof przez pomiar TTL), excalibur, packETH, gspool i ipmagic (generatory pakietów), fragroute (fragmentacja pakietów), hunt (przechwytywanie ruchu TCP), macof (zalewanie switch-ów adresami MAC)
Tunelowanie	<code>/usr/bin/tunnels/</code>	cryptcat (szyfrowany netcat), httptunnel (tunelowanie danych przez HTTP), icmpshell (tunelowanie danych przez ICMP), netcat (uniwersalne narzędzie dla sieci TCP), shadshell (tunelowanie danych poprzez UDP), stegtunnel (ukrywanie danych w nagłówkach TCP/IP), tcpstatflow (wykrywanie tunelowania).
Narzędzia do oceny zagrożeń	<code>/usr/bin/vuln-test/</code>	IRPAS (Internet Routing Protocol Attack Suite), chkrootkit 0.43: look for rootkits, clamAV (skaner antywirusowy), exodus (audytor aplikacji WWW), nbtscan (skaner sieci SMB), ncpcquery (skaner serwerów NetWare), skanery nessus, nmap.
Narzędzia dla sieci bezprzewodowych	<code>/usr/bin/wireless/</code>	airsnarf, airtsnort (sniffer dla sieci 802.11b), airtf (analyzer wydajności sieci 802.11b), kismet i kismet-log-viewer (sniffer sieci Wi-Fi), macchanger (zmiana adresu MAC), wellenreiter (wykrywanie i audyt sieci 802.11b)