NESSUS – SSH – FSTAB – MAKROPROCESOR M4 – MOTION – LOGO – GORKY 17

cena 99 Kč / 149 Sk
Květen – 05/2006

LinuxEXPRES

OPRAVDOVÝ LINUXOVÝ MAGAZÍN

Bezpečnost a zálohování

Zbavte se crackera
Nedejte mu šanci

SSH není terminál
Naučte se jej používat

Pohlídejte si zaměstnance
Motion zachytí pohyb

GNOME opět v nové verzi
Makroprocesor M4 umí pomoci
Smažte disku navždy paměť
Jádro je stále ve vývoji

Deset ukázkových stran tohoto čísla najdete na www.linuxexpres.cz

Elektronické předplatné: LinuxEXPRES také jako PDF!

GNOME 2.14 – čerstvý závan

Přestože se jedná o dost fádní označení, myšlenka, že nová verze „pouze“ opravuje chyby a přináší pár úprav fasády, by byla opravdu chybná. Postupem času, během vývoje, nám lidé kolem GNOME poodhalovali novinky, které se v této verzi mají objevit. Protože to byly změny dost zásadní a mnohými vytoužené, dne D určeného na 15. března jsme se nemohli dočkat. V tomto článku nastíním, o jaké novinky se jedná. David Kovář.

O AUTOROVI

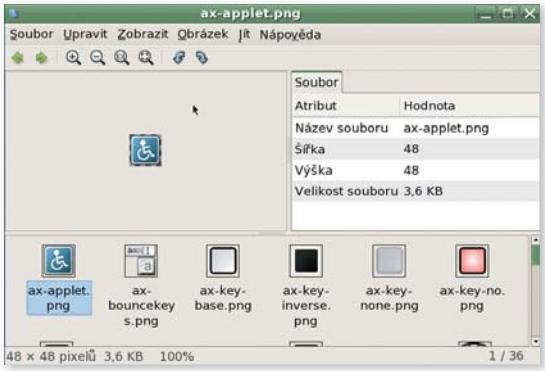
David Kovář (*1981) je student ČVUT FEL v oboru výpočetní technika. Protože škola a práce zaberou spoustu času, o to více si pak užívá florbalu, jízdy na kole, přírody, fantasy a sci-fi literatury, ministrantů, kamarádů a ze všeho nejvíce samozřejmě své dívky. Motto: Život je pes a pes je nejlepší přítel člověka!

Pokud bychom se podívali na novinky mezi aplikacemi, nejmarkantnější změnu pravděpodobně zaznamenal GnomeMeeting. Od nynějška si totiž říká Ekiga (jelikož navazuje na GnomeMeeting, začíná se rovnou verzí 2.00). A změna názvu v sobě nese obrovskou změnu v programu samotném. Byla implementována plná podpora protokolu SIP, včetně podpory STUN serverů umožňujících komunikovat přes firewall nebo NAT. Teď už stačí mít jen dostatečně tlustý drát k internetu a můžete svobodně telefonovat nebo pořádat videokonference.

URL článku:
www.linuxexpres.cz/06a5

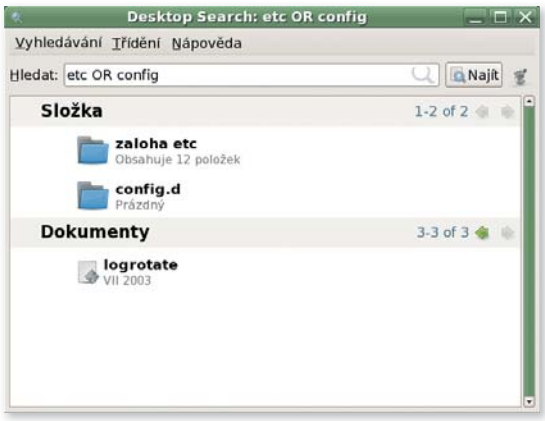
Novinky pro uživatele

Před jistým časem, někteří si na to určitě pamatují, se o GNOME říkalo, a jistě ne neprávem, že je rychlejší a méně hardwarově náročné než jeho nejbližší „konkurent“ KDE. Jak šel čas, vývojáři GNOME na tento prvek trochu pozapomněli a z prostředí se stal pěkný bumbrlíček. Dokonce bylo značně ohroženo jeho nasazení v embedded aplikacích; tomu bylo třeba učinit přítrž.



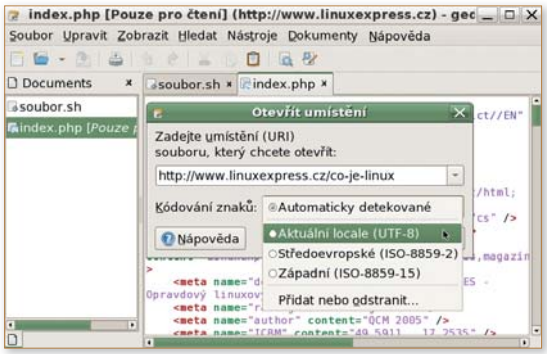
Náhled na obsah celého adresáře v prohlížeči obrázků

A přítrž to byla dost razantní. Snad proto, že bylo dost míst, kde optimalizovat; – ale jedno je jisté. Zrychlení aplikací je opravdu vidět. Až dvacetinásobné zrychlení oproti předchozí verzi, jak je uváděno na webových stránkách u programu LogViewer, jsem sice při testování nezaznamenal, ale stačí spustit okno Nautilusu, Geditu nebo GNOME Terminalu a budete mile potěšeni znatelně rychlejší odezvou. Obzvláště pokud pracujete na pomalejším počítači nebo notebooku – jako například já.



Složitější vyhledávání pomocí Beagle

Dvou drobných změn naznal i okenní manažer Metacity. Pravděpodobně všichni si hned při prvním vyzkoušení všimnou, že okýnka se teď na sebe umí nalepovat. Najedete-li s oknem poblíž nějakého jiného, okno se automaticky přilepí přímo na hranu vedlejšího okna. Stejně tak to funguje i při přetažení k okraji plochy. Druhou změnou, která už není tak viditelná, je, že pokud budete mít nějakou aplikaci spuštěnou vzdáleně, objeví se v titulku okna hned za názvem aplikace, na jakém stroji fyzicky běží. To si určitě oblíbí administrátoři, kteří vzdáleně spravují systémy pomocí GNOME. Od této chvíle už jim nebude hrozit, že si okýnka popletou.



Otevírání vzdálených dokumentů v gedit

Dialog a systém pro vyhledávání v souborech také doznal změn. Od této verze je možné hledané fráze včetně výsledků ukládat a později zase načítat. Pokud se nebojíte frameworku Mono, je vyhledávací dialog připraven také pro náruživého čmuchala Beagle. Navíc proběhl lehký facelift pod taktovkou GNOME HIG. Pro někoho se může jednat krok zpět, vše je ale v duchu hesla „Simply works!“

Ve chvíli, kdy budete v úzkých a budete se rozhlížet po pomoci, střetnete se s další novinkou, kterou potkalo vyhledávání v nápovědě Yelp. Zadaný výraz

se to nestane. Nutno ještě podotknou, že je dobré parametr `-e` uvádět až jako poslední, protože spouštíte-li nějakou aplikaci/příkaz a předáváte jí nějaké další parametry, tak s tím XTerm počítá, a ve chvíli, kdy narazí na `-e`, posílá vše další jako parametr aplikaci. V `.Xresources` se místo parametru `-hold` používá `hold` s hodnotou true.

Ještě chvíli zůstaneme u příkazu `ps aux`, jehož výstup je obvykle velmi dlouhý a ve většině situací nám přesáhne hranice jedné obrazovky a my tedy musíme nějak zajistit, že to, co se nevejde na obrazovku, se někam uloží a budeme se na to moci ještě podívat zpětně. K tomuto poslouží parametr `-sl`, tento jako hodnotu očekává počet řádků, které si má Xterm pamatovat. Standardně je tato hodnota nastavena na 64, ale není problém ji změnit. Určitě si říkáte: „K čemu mi ale je, že mám uloženo několik řádků zpět, ale nemůžu se k nim dostat?“ Odpověď je jednoduchá, parametr `-sb`, který nám spustí scrollbar (táhlo známé například z webových prohlížečů). Musím ale připomenout, že scrollbar nemusí být nutně zapnut, pokud máte nastavené kolečko u myši, dá se „scrollovat“ pomocí něho. K nastavení scrollbaru se v `.Xresources` používá volby `scrollBar` s hodnotou true pro jeho zapnutí.

Pokud se vám nelíbí pípání, které terminál běžně vydává při chybách, můžete si pomocí parametru `-vb` zapnout tzv. „visual bell“, tj. nebude vám už PC pípat, ale bude vám blikat XTerm. Já osobně nejraději vypínám jak speaker, tak visual bell, protože jeden je nepříjemný pro uši, druhý po oči. Pro zapnutí visual bellu se v `.Xresources` používá parametr `visualBell` s hodnotou true.

Nyní přistoupíme k „grafickým vychytávkám“. Nelíbí-li se vám ten klasický titulek okna (většinou je tam napsáno XTerm nebo nějaký podobný nápis), můžete si jej pomocí parametru `-T` změnit, ale dávejte si pozor na víceslovné titulky, které je třeba dát do uvozovek. Další vychytávkou je mezera mezi textem uvnitř terminálu a jeho okrajem (na obrázcích je použita hodnota 10), tu určuje parametr `-b`. Vadí vám věčné ruční

```
XTerm*locale:           false
XTerm*curses:           true
XTerm*cursorBlink:      true
XTerm*cursorColor:      red
XTerm*cursorOffTime:    100
XTerm*cursorOnTime:     200
XTerm*popOnBell:        false
XTerm*visualBell:       false
XTerm*messages:         true
XTerm*underLine:        true
XTerm*metaSendsEscape:  true
XTerm*ctrlFKeys:        12
XTerm*color256:         true
XTerm*color1:           darkred
XTerm*color3:           orange
XTerm*color4:           navyblue
XTerm*color5:           magenta
XTerm*color6:           deepskyblue
XTerm*color7:           white
XTerm*background:       black
XTerm*title:            Terminal
XTerm*foreground:       white
XTerm*font:             -*-terminus-medium-*-*-*-14-*-*-*-*-*-iso8859-2
                                                        24,1          16%
```

ATerm: .Xresources

roztahování okna XTermu pro vaši vlastní potřebu? Nastavte si ho sami! Provádí se to parametrem `-geometry`, ten jako hodnotu očekává šířku a výšku ve znacích oddělenou písmenem x. Pokud si tedy chcete spustit XTerm se standardní velikostí okna 80x25 řádků, použijete příkaz `xterm -geometry 80x25`. V `.Xresources` se titulek okna nastavuje pomocí parametru `title`, parametr `-b` se nahrazuje `internalBorder` a velikost okna se nastavuje pomocí parametru `geometry`.

Parametr `-tb` spustí velice užitečnou utilitku (ono je to vlastně menu), pomocí které si můžete interaktivně nastavit některé funkce a vlastnosti XTermu přímo za běhu. Tyto se ovšem nikam neukládají, takže je to spíše jenom tak na vyzkoušení, co jak bude vypadat a podobně.

ATerm

Budu se snažit popisovat parametry ATermu ve stejném pořadí jako u XTermu, abyste měli možnost srovnat si rozdíly, popřípadě podobnosti. V závorce parametry pro soubor `.Xresources`. Začneme tedy nastavováním pozadí a popředí (barvy textu). Pozadí se nastavuje pomocí `-bg` (`background`) a popředí pomocí `-fg` (`foreground`), takže to není až zase tak odlišné, že. Hodnoty se pro tyto parametry používají ty stejné jako u XTermu (názvy barev). K nastavení písma se používá, stejně jako u XTermu, parametr `-fn` (`font`).

Co se kurzoru týče, tak pro ATerm se jeho barva nastavuje pomocí parametru `-cr` (`cursorColor`), který jako hodnotu očekává barvu kurzoru. Blikání kurzoru ATerm bohužel nepodporuje.

Ke spuštění programu pod ATermem se používá stejný parametr jako u XTermu, tím je `-e`,

XTerm je vyvíjen člověkem, jehož jméno je Thomas E. Dickey, ten začal s vývojem už v roce 1995 a pokračuje v něm prakticky dodnes. V dnešní době je XTerm prakticky základní výbavou X Window Systemu a ve většině dnešních distribucí patří mezi jeho závislosti. ATerm je zkratka od „AfterStep Terminal Emulator“ a jak už z názvu vyplývá, je součástí okenního správce AfterStep.

Soubor `.Xresources` pochopitelně slouží k nastavení mnoha jiných aplikací, hlavně těch starších, nejenom terminálů. Prostředky Xresources jsou ovlivňovány programy psané např. v rozhraní OpenMotif.

Nezapomeňte, že při jakékoliv změně souboru `.Xresources` je potřeba provést jeho opětovné načtení do paměti pomocí příkazu `xrdb ~/.Xresources`.

```
 Levý    Soubor    Příkaz    Nastavení    Pravý
<-/                    v>  <-/                    v>
 Jméno          Délka  Modifikace   Jméno          Délka  Modifikace
/bin             4096 16.úno 17:41 /bin             4096 16.úno 17:41
/boot            4096 11.úno 20:30 /boot            4096 11.úno 20:30
/dev            13620 22.úno 06:51 /dev            13620 22.úno 06:51
/etc             4096 24.úno 06:15 /etc             4096 24.úno 06:15
/gamer           4096 24.úno 23:30 /gamer           4096 24.úno 23:30
/home            4096 31.led 15:51 /home            4096 31.led 15:51
/html            4096 19.úno 19:25 /html            4096 19.úno 19:25
/lib             4096 16.úno 05:26 /lib             4096 16.úno 05:26
/lost+found     16384 29.led 21:54 /lost+found     16384 29.led 21:54
/mnt             4096 21.úno 17:16 /mnt             4096 21.úno 17:16
/opt             4096 14.úno 11:24 /opt             4096 14.úno 11:24
/proc               0 20.úno 20:48 /proc               0 20.úno 20:48
/root            4096 16.úno 18:06 /root            4096 16.úno 18:06
/sbin            4096 19.úno 18:33 /sbin            4096 19.úno 18:33
/sys                0 20.úno 20:48 /sys                0 20.úno 20:48
/bin                               /bin
Tip: V seznamu adresářů můžete mít i často navštěvované ftp servery. Zkuste C-\.
motyl@gentik / $
 1Nápověd 2MenuUž 3Prohlíž 4Editace 5Kopirov 6Přesun 7NovýAdr 8Smazat 9HlMenu 10Konec
```

ATerm: . Midnight Commander

Jaké bylo LinuxEXPO 2006?

Akce proběhla ve dnech 10.–12. dubna v pražském hotelu Olympik. Stejně jako v předchozích ročnících doprovázela výstavu konferenční část. Prostor byl věnován také otevřeným projektům. Letos poprvé se při LinuxEXPU pořádala také konference Open Government 2006. Bohdan Milar.

V příjemných prostorách přízemí hotelu Olympik, které jsme znali již z loňska, byly k vidění prezentace na téměř čtyřech desítkách stánků. Šest z nich bylo sdruženo v sektoru nazvaném *Free & Open Zone*, kterou letos organizoval Liberix, o.p.s. Vedle „známých firem" (CZilla, Danix, KDE, Slax) byly k vidění i projekty nové (GAVANET, openSUSE).

Sedící pánové: Tristan Nitot, vpravo Michal Franěk

Z komerčních prezentací byly k vidění různá serverová řešení, informační systémy, zálohovací software, antiviry apod. Potěšila přítomnost prodejců literatury a linuxových suvenýrů v podání Root.cz. Naopak zamrzela nepřítomnost tradičních linuxových firem, jejichž pověst zachraňovala jen QCM nabízející naštěstí celou škálu distribucí pro konečné uživatele.

Pondělí bylo již tradičně vyhrazeno jako *business day*, tedy pro odbornou veřejnost. V hlavních sálech probíhaly přednášky hlavního partnera (IBM), v nedalekém hotelu Čechie konference Open Government 2006 organizovaná Ministerstvem informatiky ve spolupráci s OSS Aliancí.

V pondělí jsme také zaznamenali větší výskyt VIP. Nejprve výstavní plochu navštívila ministryně informatiky a zastavila se u několika stánků, včetně Free & Open Zone a QCM. Druhou významnou návštěvou byl prezident Mozilla Europe, *Tristant Nitot*, který k nám vážil cestu z Paříže.

Vedle samotného LinuxEXPA se v inkriminovaných dnech v Praze uskutečnily také nejméně tři akce komunitní. V pondělí to byly schůzka CZLUGu a Mozilla Party (samozřejmě za účasti pana prezidenta). Úterní večer se pak nesl v duchu historicky první Mandriva Party (která navázala na loňskou, historicky poslední, Mandrake Party).

Výstaviště bylo v úterý a středu přístupno široké veřejnosti. Především v dopoledních hodinách tak obsluha některých stánků jen stěží stačila uspokojovat zájem návštěvníků o předváděné exponáty a prodávané či rozdávané suvenýry.

A nejlepší přišlo nakonec. Středeční odpoledne bylo v sálech rezervováno pro přednášky z oblasti otevřených projektů. Zájemci tak vyslechli informace o Liberixu (B. Milar), Freenetu (Z. Štěpánek), vývojové platformě Mozilla (D. Majda), Performance tunning linuxového serveru (T. Matějíček). Tahákem byly především XGL jakožto desktop zítřka (v podání J. Bence), tvorba a renderování 3D grafiky v Blenderu (M. Polčák) a nové technologie v Danixu (D. Pravec).

Co říci závěrem? Snad jen, že může litovat každý, kdo letos nepřijel. Již nyní se těšíme, že hlavní organizátor, firma Exponet, připraví v dalším ročníku nějaké zajímavé novinky. Rád bych na tomto místě poděkoval také všem partnerům, sponzorům a dobrovolníkům, bez kterých by letošní LinuxEXPO nebylo tak dobré. ■

Ministryně informatiky Dana Bérová u stánku QCM s.r.o., vlevo ředitel QCM s.r.o. David Horký

O AUTOROVI

Bohdan Milar (*1976) vystudoval Vysokou školu ekonomickou v Praze. Pracuje v obecně prospěšné společnosti Liberix. Unixové systémy používá od roku 1997. Má rád Bash, FreeMiNT a LaTeX.

URL článku:
www.linuxexpres.cz/06d5

RootKit – Dříve se jednalo o program, jenž byl využíván k získání větších uživatelských práv v systému (obvykle superuživatelských). Dnes rootkity slouží především k umístění trojských koní a různých keyloggerů do systému, kde skrytě monitorují činnost uživatele.

DoS – *Denial of Service* čili odepření služby. DoS útok je způsobem narušení bezpečnosti počítačového systému. Většinou se provádí odesláním velkého množství požadavků (současně z několika počítačů), čímž dojde k zahlcení služby, kterou oběť – v našem případě server – není schopna obsloužit.

Shellcode – kus kódu, obvykle napsaného v assembleru, který je díky chybě proveden vlánkem napadeného procesu. Často se využívá chyby přetečení zásobníku (buffer overflow). Obvykle spustí příkazovou řádku (shell) s vyššími právy (právy napadeného procesu) – ať už na konzoli, nebo vzdáleně. Právě proto je nutné spouštět démony s nejnižšími možnými privilegii.

Backdoor – zadní vrátka. Obvykle nějaká služba (telnet, ssh), kterou se cracker dostane na systém v případě, že bude přímá cesta zablokována (např. administrátor průnik objeví, změní heslo, zruší vytvořený účet). Backdoory jsou crackery v systému pečlivě skryty.

(například přes špatně napsané PHP skripty). Zapomenout bychom určitě neměli ani na soubor `/var/log/xferlog`, kam většina FTP démonů loguje veškeré pokusy o přístup a přesun souborů.

V případě, že náš server neslouží jako SMTP brána pro tisíc klientů, určitě také nakoukneme do souboru `/var/log/mail.log` a do adresáře `/var/spool/mqueue`. V lepším případě narazíme na poštu, kterou cracker nestačil odeslat. Mohla by vám v budoucnu pomoci při jeho vystopování.

Odkud jsi, cizinče?

Pokud jsme měli štěstí a vypátrali IP adresu, ze které se cracker nabourал do našeho serveru, je na čase zjistit, s kým jsme měli tu čest. Nejprve se pokusíme pomocí příkazu `dig` zjistit, ze které domény byl proveden útok. Napíšeme tedy do konzole `dig -x 195.39.10.82` a odpověď bude vypadat následovně:

```
...
;; QUESTION SECTION:
;82.10.39.195.in-addr.arpa.        IN     PTR

;; ANSWER SECTION:
82.10.39.195.in-addr.arpa. 129559 IN     PTR
  ippavlova.fofrnet.cz.

;; AUTHORITY SECTION:
10.39.195.in-addr.arpa. 252647    IN     NS
  uroboros.fofrnet.cz.
10.39.195.in-addr.arpa. 252647    IN     NS
  server1.gts.cz.
...
```

Pro nás je podstatná sekce začínající textem `;; ANSWER SECTION:`. Ihned pod těmito slovy je zapsaná hledaná IP adresa a k ní i patřičná doména. V našem případě se jedná o doménu *fofrnet.cz*. Do webového prohlížeče zadáme adresu *fofrnet.cz* a pokusíme se najít kontakt na správce dané počítačové sítě.

Bohužel ne všechny IP adresy patří do některé domény. I pro tento případ existuje řešení. Pomocí standardního programu `whois` se pokusíme najít *abuse kontakt*, případně alespoň vlastníka patřičného rozsahu. Do terminálu přitom stačí napsat magické `whois 195.39.10.82` a odpovědí nám bude

```
...
person:         Milan Kozak
address:        FOFRnet Spol. s R.O.
address:        I. P. Pavlova 69
address:        Olomouc
address:        779 00
address:        The Czech Republic
phone:          +420 775 77 88 37
e-mail:         kozak@fofrnet.cz
nic-hdl:        MK4335-RIPE
source:         RIPE # Filtered
...
```

Jak sami vidíte, máme před sebou jak přesnou adresu ISP tak i e-mail a telefonní číslo. Nezbývá než kontaktovat protistranu a potrestat útočníka.

Pár slov závěrem

Článek rozhodně není seznamem všech postupů, které útočníci používají. Snažil jsem se vám ukázat nejčastější techniky ukrytí crackera v systému. Zajímavostí může být, že někteří „vetřelci“ váš systém sami částečně „záplatují“ - snižují riziko napadení serveru dalším crackerem, a tím tak prozrazení sebe sama.

I přestože žádný server nelze stoprocentně ochránit proti napadení, snažte se dodržovat základní zásady bezpečnosti. Používejte pokud možno šifrované protokoly a silná hesla, udržujte svůj systém neustále aktuální, sledujte bezpečnostní konference a pokuste se nainstalovat některý z IDS - na internetu jsou jich desítky. ■

Hacker, či cracker?

Některé z vás možná trápí, proč v textu používám slovo *cracker* namísto často používaného a nesprávně zažitého slova *hacker*. Dovolil bych si ocitovat část svobodné encyklopedie Wikipedia, jež dává této hádance poměrně jasnou odpověď (*http://cs.wikipedia.org/wiki/Hacker*).

„Jako hackeři byli původně označováni počítačoví specialisté, programátoři s detailními znalostmi vnitřností systému či obecněji lidé, kteří se zajímali, jak přesně věci fungují. Postupem času se však tento termín začal používat pro počítačové zločince a narušitele počítačových sítí, pro které však existuje přesnější termín cracker. Dnes jsou oba pojmy často zamlčovány a jako pojem blízký původnímu významu se používá také termín geek.“

ODKAZY

Bob Toxen: Bezpečnost v Linuxu – prevence a odvrácení napadení systému, ISBN 80-7226-716-7, Computer Press, Brno 2003

http://www.linuxexpres.cz/jon-erickson-hacking-umeni-exploitace

http://www.linuxexpres.cz/bob-toxen-bezpecnost-v-linuxu-prevence-a-odvraceni-napadeni-systemu

Užitečné knihy a jejich recenze

http://www.lids.org

http://www.tripwire.org

http://sourceforge.net/projects/aide

IDS a nástroje pro kontrolu integrity systému

http://www.securityfocus.com

http://www.linuxtoday.com

http://www.lwn.net

Security portály

FTP, FTPS a sftp... Kdo je kdo?
FTP je starý protokol orientovaný na přenosy souborů. Kvůli svému věku není nikterak odolný proti útokům a navíc představuje kvůli svému principu fungování (dynamické otevírání nových portů pro přenos dat) bezpečnostní riziko i v případě, že server poskytuje pouze anonymní přihlášení, kde nám úniky hesla nevadí. Většina bezpečnostních příruček je v otázce instalace FTP serveru rezolutní – neinstalovat. A pokud už je to nutné, spouštět server v chrootu a povolit pouze anonymní přístup. FTPS je klasický FTP protokol, který jde přes bezpečnou vrstvu SSL/TLS, ale jeho popis už je mimo rámec tohoto článku. A poslední pojem `sftp`, to je uživatelský program, který se ovládá stejně jako program FTP, ale uvnitř používá výhradně protokol SSH a s protokolem FTP jako takovým nemá vůbec nic společného. Jeho funkčním ekvivalentem je program `scp`, který se zase ovládá stejně jako program `cp`.

X Window System
Opakování je matkou moudrosti, takže: X Window System (zkráceně X) je nejrozšířenější grafické prostředí pro unixové pracovní stanice. Přes svoje nedostatky až do dnešních časů nenašlo konkurenci. Architektura systému X je obrácený klient/server. Obrácený proto, že X server je aplikace běžící na klientském počítači, která se stará o vykreslování grafických prvků. Zatímco X klient je aplikace, která může běžet na stejném nebo vzdáleném počítači a která žádá X server o vykreslování. Komunikují spolu přes protokol X11, který má vážné bezpečnostní nedostatky a ani směrování přes SSH nemusí být v některých případech dostačující. Alternativou je použití VNC (*Virtual Network Computing*), které vyžaduje pouze jediné připojení a je tedy jeho tuneling přes SSH daleko jednodušší. Navíc umí propojit X11 s Windows, takže můžete mít na své unixové stanici zároveň váš desktop z Windows a naopak.

Automatické přihlášení pomocí ssh-agent

Bohužel málo koho přesvědčíte k tomu, aby místo relativně krátkého hesla zadával delší passphrase. Ale naštěstí SSH poskytuje způsob, jak to odstranit. Jednak můžeme zvolit prázdnou passphrase, ale to není moc bezpečné. Mnohem lepší je využít služeb ssh-agenta. Ten se zavede do paměti a v okamžiku, kdy SSH potřebuje rozšifrovat privátní klíč, zeptá se agenta. Ten načte zašifrovaný klíč, pomocí passphrase jej rozšifruje a výsledek opět vrátí SSH. Důležité je, že passphrase nikdy neopustí počítač a dokonce ani samotného ssh-agenta.

Bohužel samotné spuštění agenta není triviální. Jako nejlepší metoda se mi osvědčilo přidat do startovacího skriptu (např. `~/.bashrc`) následující příkaz: `ssh-agent $SHELL`.

Poté již všechny procesy SSH již budou potomky tohoto ssh-agenta, který nastaví odpovídající systémové proměnné. Pokud vás zajímá jaké, spusťte toto

```
michal@localhost ~ $ ssh-agent
SSH_AUTH_SOCK=/tmp/ssh-QAeWx15806/ ↵
  agent.15806; export SSH_AUTH_SOCK;
SSH_AGENT_PID=15807; export SSH_AGENT_PID;
echo Agent pid 15807;
```

Alternativním způsobem spuštění je tedy příkaz: `eval `ssh-agent`.`

Pokud pracujeme v grafickém režimu, bývá nejlepší spouštět `ssh-agent` již při startu X serveru. Proto je dobré spuštění napsat do souboru `/etc/X11/xinit/xinitrc`, anebo do `~/.xinitrc`. Každá distribuce má trochu jiné startovací skripty X serveru, ale ve všech bývá řádek jako `exec /bin/sh "$HOME/.xinitrc"`. A ten změňte na

```
exec /usr/bin/ssh-agent '/bin/sh ↵
  "$HOME/.xinitrc"'
```

Nevýhodou je, že se při pádu ssh-agenta musíte odhlásit z X serveru a znovu přihlásit. Když jsme ve fázi, kdy jsme úspěšně spustili ssh-agenta, můžeme do něj zavést passphrase. K tomu slouží program `ssh-add`:

```
michal@localhost ~ $ ssh-add
Enter passphrase for /home/michal/.ssh/id_rsa:
Identity added: /home/michal/.ssh/id_rsa ↵
  (/home/michal/.ssh/id_rsa)
```

Od této chvíle už nemusíme programu `ssh` (ani `scp`, `sftp`) zadávat heslo. Agent a klíče provedou bezpečné přihlašování s minimem námahy. Také jsme vyřešili problém používání SSH ve skriptech a v cronu.

```
michal@localhost ~ $ ssh ↵
  uzivatel@server.domena.com
Last login: Mon Mar 27 21:43:11 2006 ↵
  from gateway.isp.com
uzivatel@server:~$
```

Navíc agent umí další skvělou věc, a to je směrování. Pokud to mají klienty a servery povolené, můžeme se snadno přihlásit ze serveru na další server, přičemž identitu ověří agent na lokálním počítači. Pouze je nutné, aby další server měl uloženou kopii veřejného klíče.

```
uzivatel@server:~$ ssh novy-server
uzivatel@novy-server~$
```

Závěrem

Představili jsme si SSH a možnosti jeho použití. Navzdory délce tohoto článku jsme vynechali mnoho věcí, jako jsou hashovací algoritmy, algoritmy RSA/DSA pro technologii klíčů, různé šifrovací metody jako 3DES, Blowfish, RC4 a podobně. Rovněž jsme se nezabývali nastavením SSH klienta a serveru. Ale doufám, že jsem vám SSH představil jako velice silný, bezpečný a snadno použitelný (což se někdy neslučuje s bezpečným) nástroj pro vzdálenou komunikaci po internetu. SSH samozřejmě není jediná použitelná metoda a třeba pro ochranu FTP protokolu jej není možné vůbec použít. Velká slabina i při používání klíčů je v jejich distribuci, což samotné SSH neumí a ani nemůže řešit, pokud má být pořád oním jednoduchým nástrojem. Ale díky podpoře různých způsobů autentifikace můžeme používat SSH třeba ve spolupráci s MIT-Kerberos, který mimo jiné řeší i problém neustálého kopírování veřejných klíčů. ■

ODKAZY

http://www.openssh.com
Stránka projektu OpenSSH

http://www.openbsd.org
Stránka projektu OpenBSD, tvůrců OpenSSH

http://www.openssl.org
Projekt OpenSSL

http://www.realvnc.com
Oficiální stránky VNC

http://www.tightvnc.com
Další z VNC implementací

http://web.mit.edu/kerberos/
Stránka tvůrců protokolu Kerberos na MIT

http://josefsson.org/shishi/
OpenSource implementace protokolu Kerberos

http://www.x.org
Stránky správců nejrozšířenější open-source implementace X11

http://www.iana.org/assignments/port-numbers
Seznam přiřazených portů organizace IANA

http://www.vandyke.com/technology/drafts.html
Návrhy protokolu SSH (verze 1 i 2) u IETF

http://www.faqs.org/faqs/computer-security/SSH-faq/
Často kladené dotazy

Konfigurace disků a souborových systémů

Začátečníkům může toto téma připadat obtížné, ale po rozkoukání se v systému zjistí, že má svou logiku. Stačí pochopit problematiku, prakticky si vše vyzkoušet a rázem je ze začátečníka profesionál. A aby se vám to lépe dařilo, pokusím se vám problematiku přiblížit. Jindřich Vrba.

O AUTOROVI

Jindřich Vrba (*1982) studuje počítačové systémy na Vyšší odborné škole v Liberci. Je příznivce myšlenky free softwaru a GNU. Líbí se mu Debian (hlavně díky balíčkovacímu systému a kvalitě dokumentace). Má v oblibě psaní bashových skriptů.

Vysvětlení pomocí Windows oddílu

Dejme tomu, že jste noví uživatelé Linuxu a kdysi jste používali Windows. Když jste si chtěli s kamarádem vyměnit nějaká data, připojili jste jeho disk do počítače, spustili Windows a disk se objevil pod nějakým písmenem, například `e:\`. Teď ale používáte Linux a chcete udělat to samé. Pokud používáte nějakou „uživatelsky přívětivou“ distribuci, je možné, že vám vše zařídí a data na disku najdete někde v `/mnt/` nebo `/media/`. Co ale dělat, když ne?

Nebudeme se zabývat tím, jak se to dá zařídit v různých grafických nástrojích a rovnou se vrhneme na příkazový řádek. Dejme tomu, že máme disk připojen do počítače jako *primární slave*, tím pádem ho v Linuxu najdeme jako `/dev/hdb`. Ještě je potřeba zjistit, který oddíl je ten správný. Na to budeme potřebovat vypsat všechny oddíly na disku (zde na ukázku je jen důležitá část výpisu).

```
# fdisk -l /dev/hdb
Device     Boot  Start  End   Blocks    systém
/dev/hdb1  *     1      510   4096543+  W95 FAT32
/dev/hdb2        511    1191  5470132+  W95 FAT32
```

Jak je vidět, na disku jsou dva oddíly FAT32. První je bootovací, na něm bude pravděpodobně systém, takže nás bude zajímat spíše druhý. Připojit ho můžeme třeba do `/mnt/win_data`, na to použijeme příkaz

```
# mount /dev/hdb2 /mnt/win_data/
```

(adresář `/mnt/win_data` musí existovat). Tak a oddíl je připojený a dostupný.

Disk máme půjčen na delší dobu a potřebujeme na něj každý den ukládat nějaká data. Nebudeme ho samozřejmě pokaždé připojovat takovýmto zdlouhavým způsobem, a tak si údaje zapíšeme do konfiguračního souboru. Na to je vyhrazen soubor `/etc/fstab`. Jeho struktura je jasně daná, najdete ji v rámci.

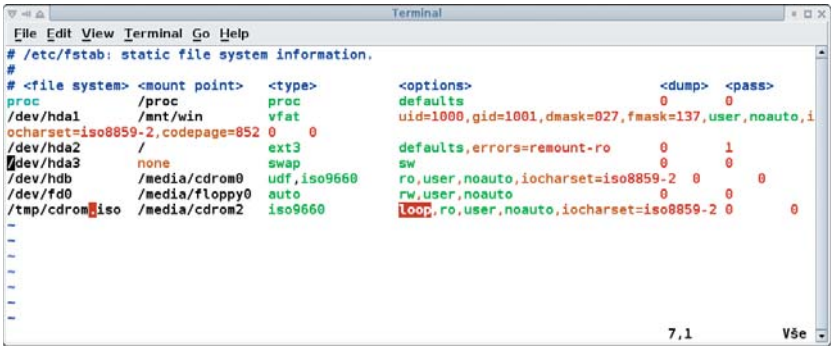
Podle tohoto pravidla bude záznam o našem FAT32 oddíle vypadat takto:

```
/dev/hdb2  /mnt/win_data  auto  defaults  0  0
```

Struktura souboru `/etc/fstab`

1. umístění zařízení
2. kam připojit
3. typ souborového systému
4. parametry připojení
5. určuje, jestli bude svazek zálohován
6. určuje, zda kontrolovat při startu

První dvě položky asi nemusím vysvětlovat. Typ souborového systému jsem nechal na hodnotě `auto`, což znamená zjišťovat automaticky. Hodnota `defaults` je výchozí hodnota pro parametry disku. Nula na páté pozici znamená, že svazek nemá být zálohován. Nula na šesté pozici znamená, že nemá být ani kontrolován. Takto záznam v `/etc/fstab` odpovídá příkazu, který jsme si ukázali před chvílí. Teď už budeme mít disk připojen vždy po startu, aniž by bylo nutné psát nějaké příkazy.



Možná jste si ale všimli, že na disk může zapisovat jen root, diakritika se nezobrazuje správně nebo máte připomínky k nastaveným právům. Také se vám nemusí líbit, že je typ souborového systému nastaven na `auto`. Takže to doopravíme následovně:

```
/dev/hdb2  /mnt/win_data  vfat  umask=0,↵
  iocharset=iso8859-2,codepage=852  0  0
```

Jak vidíte, typ souborového systému je teď zadán přímo, a to `vfat` (bylo by možné použít i `msdos`, ale délka názvů souborů by byla krácena na jedenáct

URL článku:
www.linuxexpres.cz/06k5

Soubor `/etc/kamera1.conf` pak obsahuje pouze dvě volby

```
netcam_url http://ip.adr.sitove.kamery/↵
mjpg/video.mjpg
target_dir /cesta/do/adresare/kamery1
```

Tyto soubory je nejlepší vytvořit ručně a pouze tam dodat upravené parametry nutné pro danou kameru. Vytvoření souboru zkopírováním `/etc/motion.conf` je sice možné, ale proč to dělat složitější, než to je.

`threshold ↵ hodnota`	množství změněných pixelů, který považujeme za pohyb
`noise_level ↵ hodnota`	úroveň šumu, stejně jako `threshold` umožňuje jemné doladění detekce pohybu
`pre_capture ↵ počet`	počet uložených snímků před detekcí pohybu
`post_capture ↵ počet`	počet uložených snímků po ukončení pohybu (u těchto parametrů opatrně, příliš vysoké hodnoty `pre_capture` i `post_capture` mohou značně zatížit počítač)
`gap hodnota`	dva pohyby jsou považovány za různé, je-li překročena tato hodnota (v sekundách); Motion rozděluje jednotlivé pohyby, je-li časový úsek mezi pohyby menší než tato hodnota, budou pohyby považovány za jeden a spojeny dohromady
`output_normal ↵ [on, off, first]`	při detekci pohybu ukládej také obrázky (JPG) stále (`on`), nikdy (`off`), pouze první snímek (`first`)
`ffmpeg_cap_↵ motion ↵ [on, off]`	je-li zapnuto pak (kromě videa zachycujícího celou oblast) vytvoří i video obsahující pouze pohybující se objekt – „snímky zeleného ducha“
`ffmpeg_video_↵ codec [mpeg1, ↵ mpeg4, msmpeg4]`	důležitá volba, která říká, v jakém formátu má být ukládáno video, mpeg1 vytváří soubory .mpg, mpeg4 a msmpeg4 .avi; chcete-li si však přehrát video i ve Windows bez nutnosti dodatečně instalovat příslušný kodek, použijte msmpeg4
`snapshot_↵ interval ↵ hodnota`	vytvoření pravidelného snímku v intervalu hodnota (v sekundách)
`snapshot_↵ filename ↵ formatovaci_↵ retezec`	název automatického snímku
`jpeg_filename ↵ formatovaci_↵ retezec`	název obrázků zachycujících pohyb
`ffmpeg_↵ filename ↵ formatovaci_↵ retezec`	název videa zachycujícího pohyb (doporučuji nechat výchozí hodnoty, řetězec obsahuje datum, čas, atd..)
`mail ↵ emailova_adresa`	při detekci pohybu pošle e-mail
`execute prikaz`	při detekci pohybu vykoná příkaz

Nyní máme nakonfigurováno, a tak můžeme spustit vlastní program. To provedeme příkazem `motion`. Pokud jsme nastavili `daemon on`, pak bude program spuštěn na pozadí. Teď už jen stačí zamávat do kamery a můžete si prohlédnout výsledek své práce.

Automatizujeme činnost

Nejprve bych chtěl upozornit, že následující postup není jediný možný a na stránkách projektu naleznete další. Bohužel mi nefungoval. Nicméně chyba bude zřejmě někde mezi židlí a klávesnicí. Zadáme `crontab -e` a můžeme napsat:

```
0 6 * * * /usr/bin/motion
0 21 * * * killall motion
10 21 * * * /nejaka/cesta/zpracovani
0 3 * * * /usr/bin/find /cesta/k/zaznamum ↵
  -type f -name '*.avi' -mtime +14 -exec ↵
  rm {} @reboot /usr/bin/motion
```

Po ukončení editoru dojde k aktivaci nového crontabu. Výše uvedené znamená toto: v 6:00 spusť `motion` a ukonči ho ve 21:00, ve 21:10 spusť `zpracovani` a konečně ve 3:00 smaž záznamy starší 14 dnů. Poslední záznam pak spustí `motion` při startu počítače. Skript `zpracovani` se stará o vytvoření denního snímku a smazání dále nepotřebných souborů.

Při vytvoření denního záznamu je vhodnější použít výše uvedené `cat `ls -r -t *.avi`` než `cat *`, jak je uvedeno ve FAQ projektu. Pomocí `ls` si totiž záznamy seřadíme dle času vzniku, a tak jsou ve výsledku umístěny v pořadí, v jakém byly vytvořeny.

Nyní už zbývá jenom zpřístupnit adresář s výsledným (průběžným) záznamem i ostatním počítačům – např. pomocí Samby. Počítač umístit na nějaké vhodné místo a na bednu raději napsat heslo uživatele root – pro případ, že bychom ho zapomněli. *(To je samozřejmě vtip, pozn. red.)* ■

Program neobsahuje žádné speciální ovladače pro kamery, a tak jsou podporována snad všechna zařízení rozeznaná jádrem – video4linux (např. `/dev/video0`) a síťové kamery.

Aplikaci si můžete stáhnout na stránkách projektu. Máte na výběr rpm nebo deb balíček, nebo zdrojový kód. Seznam balíčků potřebných pro instalaci programu naleznete v instalační příručce na stránce projektu.

Další dokumentaci k programu naleznete na oficiálních stránkách projektu. Velmi užitečná je stránka FAQ, kde naleznete většinu odpovědí na své otázky.

ODKAZY

http://motion.sourceforge.net
Domovská stránka projektu
http://www.mplayerhq.hu
Domovská stránka Mplayeru a Mencoderu

```
#!/bin/bash
# skript zpracovani
# zjištění aktuálního data, které se použije v názvu souboru
datum=`date +%d`
# zpracování jedné kamery, pro další kamery nutno přidat a upravit
cd /cesta/do/adresare/kamera1
#vytvoření denního záznamu
cat `ls -r -t *.avi` >> /cesta/hotovo/kamera1/video.avi
rm *
cd /cesta/hotovo/kamera1
#oprava výsledného souboru pomocí mencoderu
mencoder -noidx -o $datum.avi -ovc copy  -oac copy video.avi
rm video.avi
```

Pokud zvolíte jednu ze zde popisovaných voleb a stisknete klávesu [Enter], přejde program rovnou k mazání všech disků, které nalezne. Je jedno, zda jsou to IDE, SCSI nebo SATA disky. Neumožňuje samozřejmě mazání na jakýchkoliv přenosných médiích (flashdisky, paměťové karty apod.).

- **`nofloppy`**
  Pokud startujete DBN z CD, pokouší se DBN hledat disketu, aby na ni mohl případně ukládat log soubory. Pokud nechcete, aby DBN disketovou mechaniku hledal, použijte tento příkaz.
- **`verbose`**
  Při zadání této volby jsou automaticky vypisovány zprávy kernelu, je to vhodné, pokud máte problémy s detekcí hardwaru.

Automatický režim je výhodný právě v tom, že pak už se o program nemusíte starat, jen jej spustíte a za nějakou dobu přijdete počítač zkontrolovat. Jako optimální, co se týče bezpečnosti, se mi jeví právě metoda DoD, zvláště díky vztahu bezpečnost a rychlost. Jen pro vaši představu – úplné přemazání disku o velikosti 18 GB na notebooku s Pentiem III Mobile na 650 MHz pomocí právě této metody zabralo méně než dvě hodiny.

Jestliže chcete program spustit v interaktivním módu, stačí jen stisknout [Enter]. Objeví se před vámi rozhraní, ze kterého je možno vybrat si příslušné volby. Ovládání je vcelku jednoduché, vše se ovládá rovnou z klávesnice (což asi u textového rozhraní tak moc nepřekvapí). Pomocí klávesy [m] zvolíte příslušnou metodu pro mazání (Quick Erase, RCMP TSSIT OPS-II, DoD Short, DoD 5220-22.M, Gutmann Wipe, PRNG Stream), klávesou [v] nastavíte kontrolu mazání (Vypnutá/Poslední krok/Všechny kroky), klávesou [r] nastavíte počet průchodů. Pro výběr příslušné volby můžete využít buď kurzorové šipky nebo klávesy [j] a [k] pro posun nahoru/dolů a konečně klávesu [Mezerník] pro vybrání příslušné hodnoty ze seznamu.

Pokud jste již vše příslušně nastavili, vlastní proces spustíte klávesou [F10]. V pravé horní části jste pak informováni o době, po kterou mazání již běží, o vytížení procesoru nebo datovém toku.

Sluší se samozřejmě dodat, že program je šířen pod licencí GNU GPL a je k dispozici zdarma. Autor samozřejmě neusnul na vavřínech a neustále svůj program zdokonaluje a vytváří nové verze. Poslední verze 1.0.6 je z července 2005, jsou ovšem k dispozici i betaverze staré třeba jen několik dnů. Jak je to se stabilitou těchto verzí, nemohu posoudit. Jejich použití samozřejmě doporučuji v případě, že není váš disk správně detekován verzí 1.0.6. Protože je v betaverzi novější linuxové jádro, může být váš dříve „neživý“ hardware detekován a můžete s ním DBN použít. Autor také říká, že novější verze může na jistých kombinacích hardwaru fungovat rychleji než doposud. Máte-li se stabilní verzí problémy, stáhněte beta verzi a vyzkoušejte ji.

Svou recenzi musím zakončit konstatováním, že pro mé účely posloužil program velmi dobře a byl jsem s ním spokojen. Mohl jsem s klidem pustit pevné disky do světa bez toho, aniž bych se musel obávat toho, že by nějaká důvěrná data „prosákla“ na veřejnost. Pokud řešíte obdobný problém jako já, doporučuji DBN alespoň vyzkoušet. Je malý, levný a šikovný. ■

K dispozici jsou nástroje pro vytvoření diskety jak v Linuxu, tak i ve Windows. Verze pro CD a disketu jsou totožné. Zvláštností je i verze pro Macintosh PowerPC.

Co dalšího slibuje autor do dalších verzí? Především přidání nové metody ISAAC PRNG, podporu disků připojovaných přes USB nebo Firewire a podporu lokalizace. Každý má samozřejmě právo říci, co by chtěl mít v nových verzích.

ODKAZY

http://dban.sourceforge.net
Oficiální domovská stránka programu Darik's Boot and Nuke

http://www.linuxexpres.cz/system-rescue-cd
Článek o System Rescue CD

POJĎTE SI S NÁMI POPOVÍDAT

Již nějaký čas je pro vás, příznivce Linuxu a naše čtenáře, k dispozici konferenční místnost linuxexpres@conf.netlab.cz. V ní se můžete on-line setkávat s redakcí i mezi sebou. Můžete se podělit o své nápady, řešit nejrůznější problémy a nebo si jen tak pokecat. Třeba o životě.

Protože mnoho z vás neví, že tato místnost existuje, jak se do místnosti dostat a adresa linuxexpres@conf.netlab.cz vám může připadat více magická než srozumitelná, pokusíme se vám v následujících řádcích přístup do místnosti ve stručnosti osvětlit. Podrobný návod s popisem přístupu z mnoha rozšířených klientů pak naleznete na našich webových stránkách.

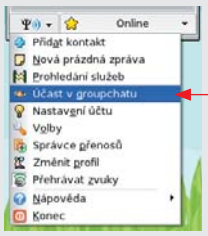
Konferenční místnost LinuxEXPRESu je víceuživatelský chat a funguje pod protokolem Jabber. Pro vstup do místnosti je nutné mít na počítači nainstalován některý z klientů, které Jabber podporují (mnoho z nich jsme popsali v minulých číslech). Mezi tyto klienty patří například Psi, Gajim, Gaim, Kopete nebo Miranda. My si v následujících řádcích přiblížíme založení Jabber účtu a přihlášení do místnosti z multiplatformního Jabber klientu Psi.

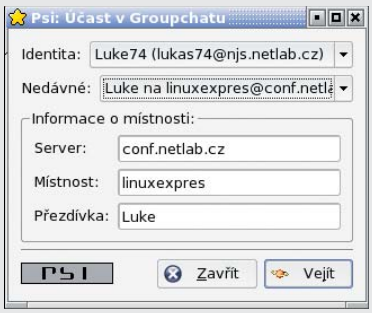
Po stáhnutí, nainstalování a spuštění Psi se vám na obrazovce objeví formulář vyzývající k otevření profilu. Pokud Psi spouštíte poprvé, musíte si nejprve profil založit. V profilu pak musíte vytvořit účet (nebo se připojit k již existujícímu).

Na rozdíl od účtů jiných systému se váš tzv. JID (Jabber identifikátor) skládá ze dvou částí. První část tvoří vaše uživatelské jméno. Druhou část pak adresa serveru. První a druhá část se stejně jako u emailové adresy odděluje znakem @. Celé JID pak vypadá následovně: username@server.com. Uživatelské jméno si zvolte libovolné. Adresu veřejného serveru pak musíte znát. V našem případě je vhodné použijeme český server njs.netlab.cz, na kterém je založena i konferenční místnost. Skutečné JID pak může vypadat následovně: lukas74@njs.netlab.cz. Poté už jen stačí, když vyplníte a potvrdíte heslo, případně nastavíte proxy a stisknete tlačítko Registrace.

Pro přihlášení do místnosti LinuxEXPRES pak v hlavním menu, které je schováno pod tlačítkem se znakem Psi a umístěno vlevo dole, vyvolejte nabídku Účast v Groupchatu. Objeví se formulář, ve kterém byste měli mít předvyplněné pole Identita. V oblasti Informace o místnosti pak do textového pole Server napište conf.netlab.cz. Do pole Místnost doplňte linuxexpres a do pole Přezdívka vepište přezdívku, pod kterou chcete být v místnosti vedeni. Poté jen stiskněte tlačítko Vejít a můžete si s námi povídat. Přejeme hodně štěstí a těšíme se s vámi na viděnou.

Redakce





Technické požiadavky
Jadro: 2.4.x alebo novšie
X Window System
Procesor: Pentium 2 200 MHz alebo lepší
Pamäť: 64 MB a viac
OSS alebo ALSA kompatibilná zvuková karta
Licencia: komerčná, 39$

Zmutovaní obyvatelia mesta okrem svojho odpudivého výzoru a novonadobudnutých deštruktívnych schopností disponujú často aj imunitou voči niektorému typu obzvlášť ničivých útokov (oheň, energetický výboj) – členovia vášho tímu si takúto vlastnosť síce zapamätajú, ale až po neúspešnom použití útoku, ktorý pre nich môže byť osudný (a aj pre vás, keďže po smrti ktorejkoľvek z postáv hra končí).

V priebehu hry sa k vašej skupine postupne pridá hneď niekoľko ďalších postáv (štyri, pokiaľ ma pamäť neklame), ktoré vám poskytnú nielen pomoc v boji, ale aj starosti navyše (musíte ich chrániť pred násilnou smrťou); okrem toho musíte počítať s tým, že vás v istom momente neočakávane opustia (a to vrátane všetkých predmetov, ktoré ste im zverili).

Ak sa vám v ľútom boji podarí prežiť, väčšinou sa uprostred spustnutého prostredia odniekiaľ ako na zavolanie objaví truhlica plná zásob, ktorú tam odložil neznámy dobrodinec, takže môžete vyraziť v ústrety ďalším chmúrnym dobrodružstvám.

Okrem hrateľnosti sa hra môže pochváliť aj solídnou atmosférou, ktorú podfarbuje na svoju dobu veľmi príjemná grafika (hlavne čo sa týka pozadí, 3D modely sú na tom o niečo horšie), hoci nižšie rozlíšenie urobí najmä počas detailných záberov a na väčších monitoroch svoje, a kvalitná hudba so stiesňujúcimi ambientnými zvukmi.

Trochu paradoxne atmosfére hry pomáha aj fakt, že traja hlavní hrdinovia nevzbudzujú príliš veľa sympatií, od fanatického veliteľa Sullivana, ktorý sa neustále oháňa rozkazmi, až po nacionalistického Poliaka Ovitza, ktorý dialóg občas spestrí výkrikom typu „Kurwa mac!“ či „I like killing!“. Ak bol toto zámer autorov hry, môžeme im rovnako ako hercom, ktorí postavám prepožičali hlasy, jedine pogratulovať. Vďaka dobre zvládnutému ponurému vyzneniu príbehu mu tak hráči odpustia aj dosť slaboduchú zápletku. Tá obsahuje hneď niekoľko zvratov, zradu, konšpiračné teórie a senzačné pseudovedecké odhalenia, ktoré však na vašej tvári môžu vyvolať maximálne úsmev pobavenia (alebo grimasu znechutenia).

Sú tu ale aj vážnejšie výhrady. Pri solídnej úrovni zábavy ponúka *Gorky 17* pomerne krátky herný čas, ktorý na jedno kompletné dohratie neprekročí 20 hodín, pričom motivácia na opakované prechádzanie príliš vysoká nie je (jednotlivé stretnutia s protivníkmi sú prakticky totožné). Obtiažnosť sa môže spočiatku javiť náročnejšia, ale po zvládnutí princípov hry a obzvlášť pri plnení všetkých nepovinných úloh a hádaniek rapídne klesá. Ku koncu hry už majú hrdinovia k dispozícii extrémne silné zbrane, takže pri zvolení správnej taktiky je cesta za víťazstvom jednoduchá.

Mnohí hráči, ktorí mali možnosť hru testovať, sa zhodli práve na tom, že najväčším problémom je nevyváženosť, keďže s kulminujúcou dejovou líniou obtiažnosť skôr klesá. Nemožnosť efektívne preskočiť často veľmi dlhé dialógy tiež v človeku nevzbudzuje práve chuť absolvovať hru po dokončení znova.

Zaujímavosťou je, že port hry trpel dlhú dobu pred vydaním množstvom technických problémov; pred nedávnom sa ale vývoja chopil nový programátor, ktorý v rekordnom čase vychytal všetky chyby, takže sa tejto obstarožnej hry napokon dočkáme.

Pre účely recenzie som použil poslednú verziu hry určenú na testovanie, pričom vydavatelia ma ubezpečili, že presne táto verzia pôjde aj do predaja, čomu by zodpovedal fakt, že som sa nestretol s nijakými nedostatkami či nestabilitou (čo sa o predchádzajúcich verziách povedať nedá). Jednou z mála výhod vysokého veku hry sú nízke požiadavky na hardvér počítača, pokiaľ je to však len trochu možné, odporúčam využiť možnosti hardvérovej akcelerácie a zapnúť v možnostiach OpenGL. Grafika ta vyzerá podstatne lepšie

Z *Gorky 17* mám zvláštny pocit. Napriek tomu, že má od dokonalosti a aktuálnosti naozaj ďaleko, sa domnievam, že si zaslúži pozornosť, predovšetkým ak dáte viac na hrateľnosť než na grafiku a ak vás zaujímajú ťahové strategické hry tohto typu (a nevadí vám, že sa hra svojou cenou mierne vymyká z kategórie pamätníckych titulov). ■

Fallout & Fallout 2
Legendárna séria postapokalyptických RPG hier z roku 1997 resp. 1998. Obe bez problémov fungujú za pomoci programu Wine, o ktorom ste sa mohli viac dozvedieť v minulom čísle LinuxEXPRESU; originálne verzie hier sa stále dajú príležitostne zohnať za výhodné ceny. Práva na tretí diel (k malej radosti mnohých fanúšikov série) vlastní spoločnosť Bethesda Softworks, autori série The Elder Scrolls.

ODKAZY

http://www.linuxgamespublishing.com
Oficiálne stránky vydávateľa pre Linux
http://www.metropolis-software.com
Stránky pôvodných autorov hry