

===== uz 17.05.2005. =====

Papildinaajums vākam

Viss, kas rakstīts šādā skriptā /Times New Roman 12 Bold/ nav grāmatas teksts bet komentāri maketētājam un tulkotājam.

Rindai

- Apache2, PHP5, MySQL4.0

Jābūt šādai (labojot uz MySQL4)

- Apache2, PHP5, MySQL4

Zem virsraksta lietderīgi likt

Otrais, papildinātais izdevums (Second edition)

Papildinājumi 1. nodaļas apakšnodaļai „Daži prieciņi”

78. Ja, lietojot Windows, kāda programma nav atinstalēta, vai arī atinstalācija nav izdevusies, bet tikai izdzēsta tās mape, ir iespējams šīs programmas ierakstu nodzēst no Control Panel\ Add or Remove Programs. To var izdarīt reģistrā (ar rīku *regedit.exe*), tur atrodot `HKEY_LOCAL_MACHINE\ Software\ Microsoft\ Windows\ CurrentVersion\ Uninstall`. Tur pēc ieraksta lauka *DisplayName* var atrast traucējošo ierakstu un uz tā ar labo peles taustiņu un *Delete*.

79. Ja interesē iegūt sīku informāciju par *Windows* sistēmas stāvokli, palaidiet komandpromtu `cmd` un tajā ierakstiet `systeminfo`. Te varēs redzēt arī visus instalētos *Windows* atjauninājumus.

80. Ja vēlaties, lai dators tīklā nav redzams arī tad, kad uz tā ir palaisti *File and Printer Sharing* un *Server* servisi, komandpromptā `cmd` uzrakstiet `net config server /hidden:yes`

81. Ja Jums traucē tikko jebkura datorā ievietota CD diska automātiska palaišanās, to var izslēgt *Policies*. *Start\ Run* ierakstiet `gpedit.msc` un tajā atrodiat *Computer configuration\ Administrative Templates\ System*, tajā sameklējiet ierakstu *Turn autoplay off* un izpildiet uz tā dubultklikšķi un logā izvēlēties šim izslēgšanas parametram *Enabled*. Kā viegli saprotams, `gpedit.msc` (*Group Policy Editor*) satur ļoti daudz noderīgu *Windows* ieregulējumu iespēju, izpētiet tās un atcerieties, ko maināt, ja gadījumā radīsies vēlēšanās atlikt atpakaļ (vai arī saglabājiat stāvokļa pierakstu `txt` failā: uz *Computer configuration* vai citas sadaļas ar labo peles taustiņu un *Export List*).

82. Gan no datora paātrināšanas, gan citu lietotāju ziņkārības viedokļa (ja ģimenes datorā katram nav savs lietotājvārds) ir interesanti atslēgt pēdējo apskatīto dokumentu sarakstu. Atkal *Start\ Run* ierakstam `gpedit.msc` un tajā atrodam *User Configuration \ Administrative Templates\ Start menu and Taskbar\ Do not keep history of recently opened documents*, uz tā dubultklikšķi un izvēlamies *Enabled*. Arī šajā sadaļā ir daudz interesanta, piemēram *Clear history of recently opened documents on exit* u.c.
83. Vēl interesants papildrīks ir *System Configuration Utility*, to palaiž *Start\ Run* ierakstot `msconfig` un izvēloties interesējošo tablapu. Piemēram, sadaļā *Startup* var paskatīt, kādi procesi tiks plaisti *Windows* starta laikā, kā arī kādu parazitisku procesu šeit var pamanīt un noņemt. Ja datoram ir vismaz 256 MB RAM, var pamēģināt tablapā *SYSTEM.INI* atvērt sekciju *386enh* un labajā pusē nospieš pogu *New*, tad izveidot ierakstu *ConservativeSwapfileUsage=1*. Tas liks sistēmai vairāk izmantot operatīvo atmiņu (RAM) un mazāk rakstīt diska atmiņas SWAP failā, kam pēc datora restarta vajadzētu uzlabot ātrdarbību.
84. *System Configuration Utility* rīks (*Start\ Run* ieraksta `msconfig`) dod iespēju atslēgt pat *Windows* ielādes attēlu, ja tas kādu mistisku iemeslu dēļ Jums traucē: sadaļā *BOOT.INI* tad ieliek ķeksi pie */NOGUIBOOT*.
85. Visbeidzot, atceramies, ka palīdzības failos vienmēr var kaut ko interesantu izlasīt.

Papildinājumi 2. nodaļas apakšnodaļai „Pēc SP2 instalācijas”

8. *Windows XP SP2* iebūvētais uznirstošo logu bloķētājs dažās lapās traucē strādāt. Tāpēc ir iespēja *Internet Explorer* ejam *Tools\ Pop-up Blocker\ Pop-up Blocker Settings* un norādām adreses, no kurām nebloķēt uznirstošos logus (tas pats atrodams *Tools\ Internet Options\ Privacy\ Pop-up Blocker*).
9. Diemžēl *Windows XP SP2* instalācija neatbrīvo no visām problēmām. Kā rāda prakse, musdienās datprā ir jābūt 3 aizsardzības programmām:
1. antivīrusa programmai,
 2. uguns mūra programmai,
 3. antispyware programmai.

Jaunums datorlietotāju apziņai ir spiegu (spyware) un reklāmas (adware) parazitprogrammu problēma, kas izpaužas tādējādi, ka *Internet* sērfošanas laikā Jūsu datorā bez lietotāja brīdināšanas tiek ieliktas sīkdatnes (cookies) un, pavirši atbildot uz jautājumiem, pat instalētas programmas, kas izspiego lietotāja *Internet* ceļus, vāc informāciju (pat kredītkašu numurus un paroles) un nosūta to hakeru serveriem, kas vai nu nosūta speciāli Jums

piemērotu reklāmu, vai arī pārdod ļaundariem kredītkaršu informāciju. Izeja varētu būt aizliegt visās *Internet* pārlūkprogrammās sīkdatnes, bet tas pagaidām radīs problēmas daudzos portālos, kuri lieto klasisko autentifikāciju.

Sīkdatnes var izslēgt *Internet Explorer* ejot *Tools\Internet Options\Privacy* iestādot uz maksimālo *Block All Cookies*, bet *Mozilla Firefox: Tools\Options\Privacy\Cookies* noņemot ķeksi no *Allow sites to set cookies*.

Ja sīkdatnes izslēgt nav iespējams sakarā ar Jūsu lietoto portālu tipu, ik pa laikam ir vēlams izdzēst visas datorā saglabātās sīkdatnes. *Internet Explorer* to var izdarīt *Tools\Internet Options\General\Delete Cookies* (veselīgi ik pa laikam arī *Delete Files*, ieliekot ķeksi pie *Delete all offline content*). Savukārt *Mozilla Firefox: Tools\Options\Privacy* spiežam *Clear Aall*.

Tāpat ir jāparaugās *Control Panel\Add or Remove programs*, vai nav parādījies kaut kas, ko mees neesam vēlējušies instalēt, piemēram, *Gator*, *GMT* u.c. Tad liekās programmas jāatinstalē. Par datorā palaistajiem procesiem var spriest nospiežot trīs pirkstu kombināciju *Ctrl+Alt+Del* n izvēloties *Task Manager*. Vēlreiz jāatgādina, ka lietotājus nevajadzētu veidot ar administratora tiesībām, un arī pašam administratoram pie datora ikdienā pareizāk ir strādāt kā parastam lietotājam *User* vai *Power User*. Tas novērsīs nejaušas nevēlamas instalācijas un citus *Windows* bojājumus.

Neraugoties uz šīm iespējām, vienkāršāks risinājums ir instalēt kādu pret-spyware programmu, piemēram, *Spybot Search & Destroy 1.3* no <http://www.safer-networking.org/en/download/> vai *Microsoft AntiSpyware beta* (grāmatas iznākšanas brīdī tai ir šāds nosaukums) no <http://www.microsoft.com/downloads/>. Pēc programmas instalācijas tā jāatjaunina ejot *File\Check for updates* un pēc tam jānoskanē dators. Šī programmiņa var glābt, ja dators ir tā inficēts, ka nedarbojas pat antivīrusa programmu apdeits, tad vispirms skanējam ar *AntiSpyware* un pēc tam tiek apdeitot antivīrusa programmu un skanējam datoru ar to. Ar abām šīm programmām dators būtu jāskanē vismaz reizi nedēļā, kā arī pirms bankas operāciju veikšanas un iepirkšanās internetā.

Papildinājumi 3. nodaļas apakšnodaļai „ZoneAlarm uguns mūra instalācija”

15. *ZoneAlarm* uguns mūra programmatūra ir regulāri jāatjaunina, instalējot tās jaunāko versiju (grāmatas otrā izdevuma sagatavošanas laikā jaunākās versijas instalācijas fails jau ir *zlsSetup_55_094_000.exe*). Ir svarīgi lai programmas sadaļas *Overview* tablapā *Preferences* ieregulējums *Check for Updates* būtu iestādīts *Automatically*. Tad atjauninājuma parādīšanās gadījumā būs paziņojums, kuram sekojot varēs lejuplādēt failu. Instalācijas fails pēc tam ir jāpalaiž, atbildot *Yes* uz jautājumiem.

Papildinājumi 4. nodaļai- jauna apakšnodaļa „IIS6 Web serveris”

57. Ja izvēlamies izmantot *Microsoft* Web serveri, tad ir jāinstalē *Internet Information Services 6* jeb *IIS6* (*IIS6* instalāciju jau aplūkojām 35. punktā, kad izvēlējāmies no tā instalēt *FTP* serveri). *Microsoft IIS6* Web serveris ir sevi labi rekomendējis kā ātrdarbīgs un drošs Web serveris, Tas ir otrs populārākais aiz *Apache*; *IIS* darbina ap 21% pasaules *Webserveru*. *IIS* ir optimizēts darbam ar Web programmēšanas valodu *ASP*, bet *Apache-* ar

PHP, kaut gan uz abiem serveriem zināmā mērā ir iespējams abu šo populārāko valodu atbalsts. Atšķirībā no IIS iepriekšējām versijām (IIS4 uz *MS Windows NT4* un IIS5 uz *MS Windows 2000 Server*), IIS6 netiek uzinstalēts noklusēti, tas ir jāpieinstalē klāt no *Control Panel/Add Remove Programs/Windows Components/Application Server/IIS*. Arī pēc šīs instalācijas Web serveris automātiski nepalaidīsies, jo tam ir nepieciešama konfigurācija.

58. Web servera konfigurācija jāveic īpaši pārdomāti un uzmanīgi, jo tieši šis serviss būs daudzu naidīgā *Internet* mākoņa uzbrukumu mērķis. Līdzīgi FTP, arī Web serveri administrē no *Internet Information Services (IIS) Manager*. Tajā atrodam *Default Web Site* un ar labo peles taustiņu izsauktā komandkartē izvēlamies *Properties*. Sadaļā *Home Directory* norādam, kur būs Web root mape un kāds ir atbilstošais domēna vārds. Uz produktīvā servera root mapei nevajadzētu atrasties C: diskā, kurā ir sistēma. Izstaigājam arī visas pārējās sadaļas, pievēršot uzmanību žurnālfailiem jeb LOG failiem, tiesībām tikai lasīt vai rakstīt un izpildīt skriptus, noklusētajai mājas lapu pirmajai lappusei (tipiski te norāda vairākas iespējas *index.htm*, *index.html*, *index.asp*, *index.aspx*, *index.php*, *default.htm*, *default.html*).

59. Ja tiek instalēts visvienkāršākais Web serveris, kurš uzturēs tikai HTML lapas, norādam tikai *Read* tiesības. Lai Web serveris darbotos, ir jābūt atļautam lietotājam- ciemiņam *IUSR_SERVERAVARDS*. Ar šo lietotāju serveris lasīs mājas lapu failus, tādēļ tam jāuzliek atbilstošas *NTFS* tiesības uz root mapi (ja mapi pārceļam uz citu disku, tiesības jāsaliek ar rokām). Visvienkāršākajā gadījumā tās ir *Read* vai *Read & Execute* tiesības. Ja kādā failā būs nepieciešams rakstīt datus, piemēram lappuses apmeklējumu skaitu, uz šo failu jābūt *Write* vai *Modify* tiesībām. Atceramies likumu: vienmēr piešķirt minimālās nepieciešamās tiesības. Tad var Web serveri palaist, šādi konfigurēts serveris varēs darbināt tikai valodās HTML, CSS un JavaScript uzrakstītus mājas lapu failus.

60. Ja ir vēlēšanās veidot dinamiskas, mūsdienīgas mājas lapas un portālus, ir jāinstalē ASP, ASPX vai PHP atbalsts un atbilstoši datu bāze MySQL vai MSSQL. Lai varētu palaist *MS Windows Server 2003* iebūvēto ASP.NET atbalstu un *FrontPage Server Extensions*, tie jākonfigurē atsevišķi (*FrontPage Server Extensions* ir lēndarbīga un mazāk droša tehnoloģija, kuru var arī neizmantot). Ja lieto ASP.NET, vispirms ir jābūt uzinstalētam *.NET Framework*, tad jānorāda paplašinājums *aspx* un jāveic pārējā konfigurācija. Ja izlemts strādāt tikai ar *Microsoft* produktiem, nopietniem risinājumiem būs nepieciešama datu bāze- nāksies vēl instalēt atsevišķu *Microsoft SQL* servera servisu. Lai to izdarītu, būs uzmanīgi jāseko instalācijas vednim un jālasa palīdzības faili. Bet atceramies likumu: neinstalēt liekus servisos, kurus neizmantos.

Papildinājumi 4. nodaļai- jauna apakšnodaļa „MS Windows Server 2003 SP1”

61. 2005. gada pavasarī iznāca ilgi gaidītā *Microsoft Windows Server 2003* pirmā servispaka (SP1). Tā serverim ir noteikti jāinstalē un, kas ir svarīgi, jāveic servera konfigurācija pēc SP1 instalēšanas. Nākotnē Microsoft plāno izlaist *Microsoft Windows Server 2003 R2* izlaidumu (šīs grāmatas otrā izdevuma iznākšanas brīdī ir tā beta versija, skat.

<http://www.microsoft.com/windowsserver2003/r2/>), kas jau saturēs sevī SP1 uzlabojumus.

Šo versiju tad arī būs ieteicams iegādāties jaunai instalācijai. Šī SP1 satur ne tikai iepriekšējos atjauninājumus, bet arī stingrāku noklusēto ieregulējumu veidošanu, uzlabotu *Windows Firewall*, *Security Configuration Wizard* u.c. SP1 prasības pret datora aparatūru tādas pašas, kā iepriekš aplūkotās *Windows Server 2003* instalācijai, bet diska brīvībai vietai priekš standartinstalācijas jābūt 1,5 GB (SP1 instalācijas fails aizņem 337230 KB).

62. No <http://www.microsoft.com/downloads/> lejuplādējam failu `WindowsServer2003-KB889101-SP1-x86-ENU.exe`. Šo failu var vienkārši palaist un uzinstalēt SP1 ar atinstalēšanas iespēju. Ja diskā maz vietas, vai arī zinām, ka atinstalēt nevajadzēs, instalāciju palaižam no komandrindas `cmd` līdzīgi kā *Windows XP SP2*: `E:\install\WindowsServer2003-KB889101-SP1-x86-ENU.exe /N /O`, kur N- nevaicot rezerves kopijas un O- pārrakstīt vecos failus nejautājot. Ir iespējams arī ieintegrēt SP1 servera instalācijas CD kopijas mapē, tad servispaku palaiž ar atslēgu `/integrate:Path`, kur `Path` ir pilnais ceļš uz instalācijas CD mapi, piemēram, `E:\install\WinServ2003`.

63. Par *MS Windows Server 2003 SP1* ir vēlams lasīt vairāk <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/servicepack/>. *Windows Firewall* (tā iepriekšējā versija saucās *Internet Connection Firewall*) ir iespējams ieslēgt tikai pēc tā konfigurācijas, citādi tas traucēs normālai servera darbībai. Piemēram, lai strādātu attālinātas administrēšanas rīki, ugunsmūrī jābūt atvērtam 445 portam. Ja ugunsmūra konfigurācija ar pirmo reizi neizdosies, ir iespēja atgriezties noklusētajā stāvoklī.

64. Pēc SP1 instalācijas lietderīgi ir ne tikai nokonfigurēt jauno ugunsmūsi, bet arī iziet *Security Configuration Wizard* jeb *SCW* (starp citu, iepriekš labo nokonfigurēts serveris strādās normāli arī ja ugunsmūri neieslēgs un minēto vedni neizies, tikai tad gan drošība nebūs maksimālā iespējamā). Šis vednis palīdzēs nokonfigurēt drošības ieregulējumus visām 50 iespējamajām servera lomām, kā arī apturēs neizmantotos servisu, bloķēs neizmantotus portus, palīdzēs izveidot drošības policiju ieregulējumus, kā arī tos atlikt atpakaļ iepriekšējā stāvoklī u.c. *SCW* nav noklusēti pieejams pēc SP1 instalācijas, tas ir jāpievieno *Control Panel\Add or Remove Programs\Windows Components*.

65. Neaizmirsīsim nepieciešamību regulāri izglītoties, to var darīt arī tiešsaistes Microsoft treniņlapā <http://www.microsoft.com/learning/mcp/offers/mcdst/>.

Papildinājumi nodaļai Literatūra

Žurnāls *BOOT.lv*, 2005. gada numuri

<http://www.microsoft.com/learning/mcp/offers/mcdst/>

Labojums Anotācijai

Vardu *MySQL4.0* aizvietot ar *MySQL4*

===== 5. nod. uz 10.05.2005. =====

Papildinājumi 5. nodaļas apakšnodaļai „MySQL instalācija un konfigurācijas pamati”

Visi, kas rakstīts šādā skriptā /Times New Roman 12 Bold/ nav grāmatas teksts bet komentāri maketētājam un tulkotājam.

1. rindkopa sākot ar 2. teikumu (ši rinda nav grāmatas teksts).

No MySQL versijām v.4.0.x, v.4.1.x, v.5.x aplūkosim stabilās v.4.0.x un v.4.1.x. Vēlams izvēlēties jaunāko stabilo versiju v.4.1.x. Ja tiks veikta pāreja no v.4.0.x uz v.4.1, datu tabulas būs jākonvertē. Lai MySQL serverim varētu attālināti pieslēgties, datorā jābūt atvērtiem TCP portiem 3306 un 1053.

Izveidosim 3 apakšvirsrakstus MySQL paragrāfam:

MySQL v.4.0.x

Zem šī paliek vecie 1.-14. punkti.

Izveidosim otru apakšvirsrakstu, kuram sekos jaunajai MySQL versijai atbilstošs teksts:

MySQL v.4.1.x

15. Šobrīd stabilā, produktīvā DBVS versija ir MySQL v.4.1.11. Pirms instalē jauno versiju, jāizlasa, vai iepriekšējā ir jāatinstalē vai var instalēt pa virsu. Pārejot no v.4.0 uz v.4.1, vecā versija ir jāatinstalē, bet sākot no v.4.1.5, var instalēt jauno vienkārši pa virsu kā apgreidu. (ja līdz šim lietota MySQL v.3.x un jāsauglabā vecie dati, vispirms jāpāriet uz v.4.0.x).

16. Ja notiek augšupatjaunināšana, vispirms paņemam datu rezerves kopijas (gan kā *Windows* bkf failu MySQL instalācijas un datu mapeēm (var tikai datu ar *MySQL Administrator* rīku, sākt. tālāk). Pirms atinstalēšanas parliecinamies, vai lietotājam `root@localhost` ir visas tiesības uz visu datu bāzu visām tabulām, kas būs nepieciešams, lai vēlāk tās konvertētu.

17. Ja ir instalēta vecā versija, to var atinstalēt gan grafiskajā režīmā (*Control panel\Add Remove programs*), gan manuāli. Otrajā variantā darbojamies *cmd* logā. Ja MySQL v.4.0.x instalēta kā serviss, to apturam un atinstalējam: `C:\> NET STOP MySQL` (ja nav serviss, tad *cmd* logā: `C:\> C:\mysql\bin\mysqladmin -u root shutdown`), nepieciešams aizvērt *WinMySQLAdmin*, ja tā palaists. Tad atinstalē veco MySQL:
`C:\> C:\mysql\bin\mysqld --remove`. Mape data atinstalējot netiek izdzēsta, jo satur datu bāzes. Pēc atinstalēšanas noteikti pārstartējam sistēmu.

18. Jauno versiju instalē ne tajā pašā mapē, kur bija vecā, bet, piemēram `mysql4_1`. Tāpat servisa vārdu vajag dot citu nekā vecais `mysql`. Ja izmantos tomēr veco, noklusēto mapi un servisa vārdu, pirms jaunās versijas instalēšanas jāiztīra reģistrs (*cmd* logā *regedit.exe*) no ierakstiem, kas satur `mysql`.

19. Instalācijai ņemam jaunākās pilnās versijas pilno (*Complete Package*) bināro failu, piemēram, `mysql-4.1.11-win32.zip`, un palaižam `setup.exe` (ja izvēlēties minimizēto *Essentials Package*, tas nesaturēs papildus iespēju komponentes un skriptus, tajā skaitā veco datu bāzu konvertēšanai; vēl ir iespēja ņemt *Noinstall Archive* un visu darīt ar rokām, bez grafiskā interfeisa).

20. Būtiska v.4.1.x. atšķirība no v.4.0.x ir tā, ka jaunajā versijā instalācija ir sadalīta divās daļās: 1) failu iekopēšana ar grafisko instalācijas vedni un 2) sekojoša konfigurēšana ar otru grafisku vedni *MySQL Server Instance Config Wizard*.

21. Instalācijas vednī izvēlamies *Custom* instalācijas tipu, izvēlamies no *Developer Components* vismaz *Scripts, Examples*, norādām mapi, kā arī to, vai vēlamies uz e-pastu saņemt MySQL ziņas. Atstājam ķeksi pie *Configure MySQL Server Now* un spiežam *Finish*. Par `my.ini` faila vietu un saturu jaunajā versijā var nedomāt- MySQL to atradīs no savas mapes.

22. Kad palaižas *MySQL Server Instance Config Wizard*, tajā varam norādīt *Standard Configuration* un justies brīvi. Ja vēlamies visu paturēt savā kontrolē, izvēlamies *Detailed Configuration* un norādam dotajam datoram atbilstošāko MySQL lietojumu, piemēram, *Server Machine*.

23. Nākamajā logā jāizvēlas MySQL datu bāzu prognozējamais lietojuma veids (iepriekšējās versijās šāda iespēja bija tikai *Linux* sistēmās). Tipiski izvēlamies *Multifunctional Database*, kas nozīmē tipisku *InnoDB* instalāciju, kas optimizēta maksimālam darbības ātrumam uz ierakstu meklēšanu, kas arī ir tipiski nepieciešamais Web lietojumos. Nākamajā solī ir iespēja mainīt arī datu atrašanās vietu, pēc tam jānorāda prognozējamais savienojumu daudzums (arī te var atstāt noklusēto DSS/OLAP).

24. Būtiski ir izlemt, vai serverim klienti attālināti varēs pieslēgties konsolē vai ar dažādiem administrēšanas rīkiem. Ja tas jānodrošina, nākas atstāt ķeksi pie *Enable TCP/IP Networking* (3306 ports).

25. Tad pārvaram valodu ieregulējumu logu un reālam serverim noteikti atstājam ķeksi pie *Install As Windows Service*, lai MySQL būtu serviss, un izvēlamies servisa vārdu, piemēram `MySQL4_1` (izstrādes datorā gan var arī noņemt ķeksi un konfigurēt kā palaižamu aplikāciju).

26. Ja ieliksīm ķeksi pie *Include Bin Directory in Windows PATH*, tad `cmd` logā tiks saprasts ieraksts `mysql` bez pilna ceļa norādīšanas (uz reāla servera drošības dēļ šo ķeksi var nelikt).

27. Ja instalējam jaunu instalāciju, atstājam ķeksi pie *Modify Security Settings* un ierakstam `root` paroli (protams, garu, kompleksu). Ja mapē data bija pirms konfigurēšanas vedņa iekopētas vecās datu bāzes, tad šo ķeksi noņemam, lai paliktu vecie datu bāzes *mysql* ieregulējumi, vecie lietotāji un viņu tiesības. Tad pabedzam vedni un MySQL serverim būtu jāsāk strādāt.

28. Vecās datu bāzes var iekopēt mapē data pa virsu jaunajām arī pēc konfigurēšanas (tad, protams, būs vecā `root` parole).

29. MySQL servisu var palaist ar `NET START MySQL4_1` un apturēt ar `NET STOP MySQL4_1`, ja tādu devāt servisa vārdu (vai palaiž `mysqld`, ja instalējām kā aplikāciju). Var lietot arī *Windows* rīku *Services*.

30. Lai varētu lietot jaunās tabulu īpašības, uz *Windows* servera, lieto gatavu skriptu. Tā palaišanai cmd logā ielogojamies MySQL ar root tiesībām:

```
C:\WebServer\mysql\bin\mysql -u root -p mysql
```

Un tad palaižam skriptu, sekojot, lai norādītu pareizu ceļu, kāds tas ir konkrētajā datorā:

```
mysql> SOURCE  
C:\WebServer\mysql\scripts\mysql_fix_privilege_tables.sql
```

Pēc skripta izpildes MySQL serviss jāpārstartē.

31. Atceramies, ka *MySQL* ir neatkarīgs serviss, un lai *Apache* modulis *PHP* varētu strādāt ar *MySQL* datu bāzēm, ir jāveic izmaiņas *PHP* konfigurācijas failā `php.ini`. Tās *MySQL* v.4.1.x ir tādas pašas kā v.4.0.x, ko apskatījām šīs instrukcijas 9., 10. punktā.

Izveidosim trešo apakšvirsrakstu, kuram sekos jaunāko MySQL drošības jautājumu apskata punkti:

Daži MySQL drošības ieteikumi

32. Ja serveris ir uz MS Windows operētājsistēmas, tam noteikti jābūt aiz uguns mūra. Uguns mūrim starp serveri un internetu nav jālaiž cauri ports 3306. 36Lietot tikai jaunākās *MS Windows Server* vai *Linux* versijas.

33 Lietot tikai stingras, vismaz 16 simbolu paroles, it īpaši lietotājam root un vismaz 6 simbolu garas, citiem lietotājiem, mācīt lietotājiem veidot kompleksas. stingras paroles.

34. Noteikt IP adreses, no kurām root var pieslēgties (phpMyAdmin slēdzas it kā no servera ārējās IP).

35. Noņemt anonīmos lietotājus.

36. Noņemt, ka lokāli bez paroles logojas.

37. Ja *Windows*, lietot tikai uz NTFS failsistēmas.

38. Par datu bāzu serveri vēlams veidot "Standalone Machine" tipa serveri.

39. Instalēt jaunāko stabilo MySQL versiju, regulāri to tajaunināt.

40. Instalējot var ielikti ķeksi pie *Root May Only Connect from Localhost* (C:\WINDOWS\system32\drivers\etc\hosts failā jābūt rindai 127.0.0.1 localhost), beta atstāt neizvēlētu *Create An Anonymous Account*.

41. Jau uzinstalētai versijai 4.1.x ierobežot administratīvo lietotāju root var šādi:

```
mysql> use mysql;  
  
Database changed  
  
mysql> DELETE FROM user WHERE user = 'root' AND host = '%';
```

```
Query OK, 2 rows affected

mysql> FLUSH PRIVILEGES;

Query OK, 0 rows affected (0.05 sec)

mysql>
```

42. Jau uzinstalētai versijai 4.1.x noņemt anonīmo lietotāju:

```
mysql> use mysql;

Database changed

mysql> DELETE FROM user WHERE user = '';

Query OK, 2 rows affected

mysql> FLUSH PRIVILEGES;

Query OK, 0 rows affected (0.05 sec)

mysql>
```

43. Atspējot TCP/IP piekļuvi no jebkura hosta (v.4.1.x versijai: *Start > Programs > MySQL > MySQL Server 4.1 > MySQL Server Instance Config Wizard* noņemt ķeksi pie *Enable TCP/IP Networking*).

44. Pieslēgties serverim var pa vecam (C:\WebServer\mysql\bin\mysql -u root) vai veidojot tuneli:

```
C:\WebServer\mysql\bin\mysql -h . -u root -p
```

45. my.ini faila [mysqld] sadaļā var norādīt serverim strādāt tikai ar kādu noteiktu IP adresi: bind-address=127.0.0.1

46. Neļaut MySQL strādāt kā privilēģētam (noklusēti) lietotājam SYSTEM, bet gan kā ierobežotam lietotājam: izveido lietotāju mysql_serveravards, aptur mysql4_1 servisu un nomaina mapes mysql tiesības, noņemot tās visiem un uzliekot tikai sev (administratoram) un šim lietotājam *Full Control*. Tad servisam mysql4_1 uzliek *Log On* sadaļā logoties ar šo mysql_serveravards lietotāju, nevis SYSTEM. Tas pasargās no iespējamās servera svarīgu failu ļaunprātīgas ielādēšanas datu bāzē (LOAD DATA INFILE '/cels/uz/slepeno/failu' INTO TABLE mydatubaze.mytabula).

46. Īpaši misijai kritisku datu gadījumā administrators var ielogoties ar šo mysql lietotāju un šifrēt data mapi pret datu zudumu.

47. Veidojot jaunus lietotājus, piešķirt tiem minimumu tiesību, piemēram:

```
mysql> GRANT SELECT, INSERT, UPDATE, DELETE ON fictional.* TO
'bob'@'192.168.1.%';
```

48. Nomainīt lietotāja root vārdu:

```
mysql> USE mysql;
```

```
mysql> UPDATE user SET user='bob' WHERE user='root';

Query OK, 1 row affected (0.19 sec) Rows matched: 1 Changed: 1
Warnings: 0

mysql> FLUSH PRIVILEGES;

Query OK, 0 rows affected (0.23 sec)
```

Labot apakšnodaļā MySQL administrēšanas vortāls phpMyAdmin 2.5.x uz 2.6.x divās vietās (127.lpp.)

MySQL administrēšanas vortāls phpMyAdmin 2.6.x

...

1. Fails phpMyAdmin-2.6.2-pl1.zip vai jaunāks ir...

Papildināt apakšnodaļu Apache instalācija un konfigurācijas pamati ar 23. punktu: (112.lpp.)

23. Neļaut Apache vai Apache2 strādāt kā privilģētam (noklusēti) lietotājam SYSTEM, bet gan kā ierobežotam lietotājam: izveido lietotāju `apache_serveravards`, aptur Apache2 servisu un nomaina mapes Apache2 tiesības, noņemot tās visiem un uzliekot tikai sev (administratoram) un šim lietotājam *Full Control*. Tad servisam Apache2 uzliek *Log On* sadaļā logoties ar šo `apache_serveravards` lietotāju, nevis SYSTEM. Tas pasargās no servera pārlūkošanas ar kļūdainu vai ļaunprātīgu php scenāriju palīdzību, piemēram, lietojot php funkciju `opendir()`.

Papildināt apakšnodaļu PHP instalācija un konfigurācijas pamati 6. punktu: (116.lpp.) ar divām rindām tā gala:

6. ...

un lai padarītu drošāku darbu ar datu bāzēm:

```
magic_quotes_gpc = Off
```