



Politechnika Warszawska
Ośrodek Kształcenia na Odległość
Zaoczne Studia Inżynierskie na Odległość
(model SP_RINT)

METODY I NARZĘDZIA INFORMATYKI

INSTALACJA SYSTEMU OPERACYJNEGO

Paweł Wnuk, Jakub Możaryn, Maciej Przybylski

WPROWADZENIE.....	2
Harmonogram zjazdu.....	2
BUDOWA KOMPUTERA PC.....	4
INSTALACJA SYSTEMU OPERACYJNEGO.....	5
Ustawienia wstępne komputera	5
Partycjonowanie.....	5
Instalacja systemu Windows XP.....	6
Instalacja niezbędnych sterowników i programów użytkowych.....	7
Podłączenie komputera do sieci	7
Zabezpieczanie naszego komputera.....	9
Aktualizacja systemu Windows XP	11
Uruchomienie i konfiguracja Zapory Systemowej Windows	11
Konfiguracja przeglądarki Internet Explorer	12
Program antywirusowy	14
Instalacja programu antyspyware	14
Dodatkowe oprogramowanie.....	15
Kopia zapasowa.....	15
Instalacja systemu Linux.....	16
Ustawienia wstępne komputera	16
Partycjonowanie.....	16
Wstępna konfiguracja systemu:	16
Instalacja dodatkowego oprogramowania.....	18
Serwer plików sieci lokalnej.....	19
Serwer www.....	28

Wprowadzenie

Szanowni Studenci

Niniejszy dokument ma na celu wsparcie Was w realizacji zadań, które przewidzieliśmy jako treść zjazdu 2. Nie będzie to opis krok po kroku tego, co macie wykonać. Zazwyczaj też nie będziemy duplikowali zagadnień, które już zostały opisane w podręcznikach do przedmiotów, których uzupełnienie stanowi ten zjazd, natomiast możecie go potraktować jako podręczny notatnik – ściągnę z nowych elementów, i wsparcie dla Waszych wykładowców. Niemniej pamiętajcie – że to głównie oni będą pomagali Wam w realizacji zadań laboratoryjnych.

Zjazd jest przewidziany jako uzupełnienie przedmiotów *Architektura Systemów Komputerowych*, *Programowanie* oraz *Algorytmy i Struktury Danych*. Dokładny podział na zadania znajdziecie poniżej:

Harmonogram zjazdu

Poniedziałek

14:00-15:30: Budowa komputera PC. W trakcie zajęć w tej części uczestnicy zjazdu składają z podzespołów klasyczny komputer PC. Ich zadaniem jest montaż procesora, pamięci, napędów dysków, etc, wraz z późniejszym przejrzaniem i ustawieniem BIOS komputera. Studenci wykonują to zadanie jako jeden zespół. Każdy ze studentów dokonuje analizy konfiguracji sprzętowej komputerów przy wykorzystaniu specjalizowanego oprogramowania, oraz proponuje rozbudowę komputerów w celu dostosowania ich do przykładowych zastosowań (komputer biurowy, stacja do grafiki, mały serwer).

15:30-17:30: Instalacja i zabezpieczenia Windows XP. Studenci w trakcie tego bloku mają za zadanie zainstalować na komputerach w laboratorium system Windows XP, skonfigurować go do pracy w domenie, oraz zainstalować dodatkowe programy zabezpieczające. W ramach przygotowania do dalszych zajęć przeprowadzona zostanie również instalacja narzędzi programistycznych firmy Borland. Blok kończy się przygotowaniem i przeprowadzeniem procesu backupu komputerów w laboratorium.

Wtorek

9:00-12:30: Instalacja serwera sieci lokalnej opartego na systemie Linux. Studenci przeprowadza pełną instalację wybranej, popularnej dystrybucji tego systemu. Następnie konfiguruje na niej serwer plików, serwer drukarek, serwer www w połączeniu z serwerem baz danych, oraz firewall, zainteresowani mogą jeszcze przeprowadzić konfigurację serwera domeny, oraz udostępniania łącza wraz z funkcjami routera (maskowanie adresów).

14:00-17:30: Wprowadzenie do programowania wizualnego. Filozofia działania graficznego interfejsu użytkownika programowanie sterowane zdarzeniami. Wprowadzenie podstawowych pojęć i mechanizmów programowania obiektowego. Środowiska firmy Borland - komponenty, właściwości, metody i zdarzenia. Metody budowy aplikacji okienkowych na drodze wizualnej. Edytor kodu i edytor formatek. Przykładowe programy.

Środa

9:00-12:30 Ćwiczenia programistyczne - budowa prostych programów wykorzystujących podstawowe komponenty wizualne. Obsługa myszy, wyświetlanie i wprowadzanie tekstu, przyciski, wywoływanie systemowych okien dialogowych. Tworzenie aplikacji wielookienkowych. Reakcja na podstawowe zdarzenia systemowe oraz od użytkownika.

14:00-17:30 Zasady budowy interfejsów użytkownika przy wykorzystaniu narzędzi typu RAD. Estetyka i funkcjonalność. Podstawowe elementy GUI i obsługujące je komponenty. Scentralizowane zarządzanie wywoływaniem i udostępnianiem funkcji aplikacji. Dostosowywanie interfejsu użytkownika. Wprowadzenie do grafiki w Windows. Pojęcia podstawowe - piórko, pędzelek, płótno. Skalowanie, buforowanie i akceleracja grafiki. Obsługa plików graficznych.

Czwartek

cały dzień (przerwa obiadowa 12:30 – 14:00): Projekt z programowania wizualnego + algorytmy i struktury danych. Przewiduje się prowadzenie trzech alternatywnych projektów, do wyboru przez studenta. Każdy projekt może być zrealizowany na poziomie podstawowym lub zaawansowanym, z użyciem złożonych struktur danych i bardziej rozbudowanych algorytmów. Projekty będą prowadzone z wykorzystaniem szczególnie przygotowanych do Zjazdu materiałów ćwiczeniowych, w tym również niektórych podprogramów, opracowanych na potrzeby tych projektów.

Piątek

9:00-12:30 Programowanie w Matlabie.

Budowa komputera PC

Nasze spotkanie zaczniemy od złożenia komputera klasy PC ze standardowych komponentów. Cała grupa będzie składać jedną stację, przy okazji zapoznając się z zasadami prawidłowego montażu komputera. Po zakończeniu tej części poprosimy, w ramach sprawdzenia waszej wiedzy, o identyfikację położenia i parametrów poszczególnych elementów jednostki PC, takich jak procesor, układ sterujący (chipset), karta graficzna, itp. Drugą częścią zadania będzie oszacowanie kosztów modernizacji laboratorium komputerowego w celu przystosowania go do realizacji określonych zadań. Korzystając z wiedzy o aktualnej konfiguracji sprzętowej jednostek, będziecie mieli za zadanie zaproponowanie elementów do dokupienia, oraz przygotowanie wstępnej wyceny całościowej modernizacji w oparciu o ceny ze sklepów internetowych.

Po zakończeniu tej części ćwiczeń, każdy z Was powinien być w stanie:

1. Samodzielnie zainstalować lub wymienić nowy podzespół w komputerze (kartę, dysk, pamięć)
2. Złożyć jednostkę centralną komputera PC
3. Oszacować koszty rozbudowy laboratorium w celu jego dostosowania do nowych zadań.

Instalacja systemu operacyjnego

Ustawienia wstępne komputera

Rozpoczynając instalację jakiegokolwiek systemu operacyjnego, musimy uruchomić komputer z dostępnego nam nośnika bootowalnego z wersją instalacyjną systemu. W zależności od tego, jaki nośnik posiadamy (CDROM, DVDROM), to nastawiamy w BIOS urządzenie odczytujące jako pierwsze w kolejce do przeszukania przez komputer po włączeniu. Użytkownicy komputerów z nowszą wersją BIOS mają ułatwione zadanie, ponieważ wystarczy, że wcisną odpowiedni klawisz opisany często słowami „BOOT Menu”. Zazwyczaj jest to F8 lub F12. W starszych lub nie posiadających tej funkcji płytach głównych, musimy przestawić w BIOS, z którego urządzenia chcemy wystartować PC. W tym celu należy w trakcie startu komputera przerwać normalną procedurę poprzez naciśnięcie odpowiedniego klawisza (Bios Award – DEL, inne: F1, F2, Esc, ALT, CTRL, CTRL+ALT+ESC) podczas wyświetlania ekranu z parametrami PC. Aby dowiedzieć się jaki to klawisz, wystarczy przeczytać informację na ekranie na samym początku uruchamiania się komputera. Gdy następuje jej szybkie zniknięcie, możemy wspomóc się klawiszem Pause (Break), albo zwykłą metodą prób i błędów. Może się zdarzyć, że mamy włączone logo producenta i mimo, że nie widać informacji podobnej do – „press DEL to enter the SETUP” - to i tak naciśnięcie odpowiedniego klawisza przerwie start urządzenia i przeniesie nas do ustawień BIOS.

Następnie należy ustawić pierwsze urządzenie, z którego chcemy uruchomić komputer. Niestety – programy uruchomieniowe nie są zestandaryzowane, każdy producent stosuje własną wersję interfejsu użytkownika, lecz najczęściej możliwość ustawienia urządzenia startowego będzie ukryta pod hasłami:

- Boot Sequence
- Boot Order
- First boot device

Klawisze do zmiany urządzenia opisane są w oknie pomocy. Zazwyczaj są to klawisze: PgUp PgDn oraz klawisz F10 do zapisania konfiguracji. Do instalacji systemu Windows XP potrzebujemy, aby nasz komputer uruchamiał się z CDROM'u.

Partycjonowanie

Zaleca się aby instalacja Windows XP była na jednym dysku a dane użytkowe na kolejnych. Warto zatem przed instalacją zastanowić się jak rozdysponować miejsce na naszym dysku HDD oraz jakiego systemu plików użyć. System Windows XP obsługuje FAT32 oraz NTFS (przy wykorzystaniu dodatkowego oprogramowania także systemy Linux-owe EXT2 i EXT3. Musimy pamiętać, że FAT ma pewne ograniczenia. Istotnym ograniczeniem jest rozmiar pojedynczej partycji - nie może być on większy niż 36GB. Natomiast system plików NTFS jest w stanie obsługiwać dyski powyżej 36GB. Posiada mechanizmy szyfrowania i bezpieczeństwa zapisu danych. Idealnie pasuje dla komputerów, na których postawione są systemy do obsługi kont różnych użytkowników oraz tam gdzie operuje się na dużej ilości i wielkości plików jednocześnie np. komputery do obróbki grafik, przetwarzania strumieni multimedialnych. Ponadto należy kierować się rozsądkiem przy tworzeniu wielkości jak i ilości dysków logicznych. Dla partycji systemowej, na której można instalować system, umieszczać dane oraz programy użytkowe można spokojnie przeznaczyć przynajmniej 15-38 GB. Trzeba pamiętać, że pulpit naszego komputera to również miejsce na dysku systemowym. Resztę dysku można podzielić według własnych upodobań.

W przypadku tego laboratorium, od razu przygotowujemy miejsce na drugi system operacyjny. W związku z tym, pierwsza partycja naszego komputera będzie przeznaczona na Windows, potem będzie obszar przeznaczony dla systemu Linux, a na koniec zamieścimy jedną partycję do wymiany danych pomiędzy tymi systemami.

Na tym etapie utworzymy tylko podstawową partycję Windows, na którą przeznaczamy 10-15 GB przestrzeni dyskowej

Do tworzenia partycji na dysku dostępnych jest wiele programów. Zaczynając od tych wbudowanych w system operacyjny dostępnych z wiersza poleceń – fdisk w systemach WIN 9X lub kreator w systemie Windows XP, po komercyjny Partition Magic, albo też freewary'owe jak Ranish Partition Manager. Generalnie różnią się one oferowanymi możliwościami, stopniem zaawansowania oraz ceną. Najlepiej na początku wykorzystać ten wbudowany w instalatora systemu.

Instalacja systemu Windows XP

Instalacja systemu (potocznie często nazywa się to stawianiem systemu na komputerze) to nic innego jak przejście przez kreator instalacji oraz odpowiadanie na kilkanaście pytań zadawanych użytkownikowi.

Procedura uruchamiania komputera do instalacji systemu:

- przygotować wszystkie płytki i dyskietki potrzebne do instalacji
- włączyć komputer
- włożyć nośnik z instalacyjną wersją systemu do napędu
- odczekać na zainicjowanie się startu
- jeśli za późno włożono nośnik to wcisnąć Enter lub Reset.

Podczas rozpoczęcia bootowania wyświetli się tekst:

„Dowolny klawisz spowoduje rozruch z dysku CD.... ”

Wciskamy dowolny klawisz. Rozpoczyna się wówczas uruchomienie instalatora systemu, i sprawdzanie konfiguracji sprzętowej.

Wszystkie możliwe klawisze do obsługi wyświetlanych komunikatów opisane są na dole na pasku u dołu ekranu.

Pierwszy krok to wybór kontrolera dysku twardego.

Służy do tego celu Klawisz F6. Zdarza się często że posiadany przez nas płyta główna ma dodatkowy kontroler RAID lub SCSI do którego potrzebne są sterowniki aby nasz instalowany system „widział” dysk twardy. Najczęściej spotyka się to na płytach firmy MSI. Sterowniki do tych urządzeń dołączane są na dyskietkach. Wkładamy wówczas tą dyskietkę do stacji. Będzie ona potrzebna za chwilę do wyboru z wyświetlonej listy dostępnych na niej sterowników. Jeśli nie mamy takiego kontrolera, omijamy ten krok (nie wciskamy F6) komputer samoczynnie przechodzi do instalacji systemu Windows.

Kolejny krok to akceptacja umowy licencyjnej.

Po akceptacji program wykrywa zainstalowany dysk twardy w komputerze. Ponieważ komputery wykorzystywane w laboratorium posiadają już wcześniej instalowany system operacyjny, w pierwszym kroku usuwamy wszystkie istniejące wcześniej partycje (korzystając z klawisza D i za każdym razem potwierdzając tą operację). Następnie zakładamy nową partycję, wciskając klawisz C a następnie wpisując w pole edycyjne jej wielkość w MB. Jako system plików wybieramy NTFS. Zaleca się, aby pierwsze formatowanie dysku było pełne (bez dopisku – szybkie). Kolejne partycje będziemy zakładali później, na razie resztę dysku zostawiamy nie wykorzystaną.

Po zakończeniu formatowania rozpocznie się proces kopiowania plików instalacyjnych na nowo utworzony dysk. Czas i postęp pokazywany jest za pomocą paska oraz liczbą procent. Po zakończeniu kopiowania komputer uruchomi się ponownie. Tym razem już z dysku twardego.

Od tego momentu komputer będzie już pracował w trybie graficznym.

Na wstępie program poprosi o ustawienie opcji regionalnych:

- język
- układ klawiatury (zalecany układ polski programisty)

Na kolejnej karcie poprosi o wprowadzenie danych osobowych właściciela.

Dla systemu w wersji OEM, najważniejszy krok to wpisanie 25-znakowego, unikatowego klucza systemu. Jest to kombinacja literowo-cyfrowa zazwyczaj w postaci nalepki umieszczona na obudowie komputera. Dla komputerów przenośnych umieszczana na spodzie.

Jeżeli nasz instalator nie poprosił o ten klucz, to wtedy mamy do czynienia ze zmodyfikowaną płytka instalacyjną dla komputerów masowo produkowanych np. laptopów. Dalej instalator zapyta nas o nazwę komputera oraz hasło dla administratora systemu (hasło to jest bardzo potrzebne jeśli chcielibyśmy nasz system reanimować lub cokolwiek poprawiać za pomocą płytki instalacyjnej)

Po wprowadzeniu tych danych system zapyta nas o poprawność godziny, daty miejsca (strefy czasowej).

Kolejny krok to ustalenie sposobu łączenia się z Internetem. Pozostawiamy ustawienia domyślne.

Po tych wstępnych czynnościach konfiguracyjnych komputer rozpocznie instalację wszystkich urządzeń i programów, do których posiada sterowniki. Ekran może migotać, ponadto komputer zresetuje się w celu uruchamiania zainstalowanych elementów.

Po ukończeniu tych działań uruchomi się kreator konfiguracji systemu, w którym będziemy mogli: ustawiać nazwy i liczbę użytkowników w systemie, dokonać aktywacji systemu lub ją pominąć (w tym momencie zalecane).

Po zakończeniu pracy tego kreatora będziemy mieli zainstalowany „czysty” system na komputerze.

Teraz pozostało nam zainstalować resztę elementów oraz programy niezbędne do prawidłowego funkcjonowania naszego komputera.

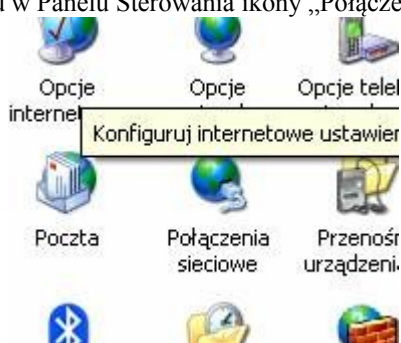
Instalacja niezbędnych sterowników i programów użytkowych

Teraz możemy rozpocząć instalowanie pozostałych elementów. Instalacje te wyglądają podobnie. Polegają na włożeniu odpowiedniego nośnika i odpowiadaniu na pytania uruchomionego z CDROM'u instalatora. Te prace najlepiej wykonywać w odpowiedniej kolejności:

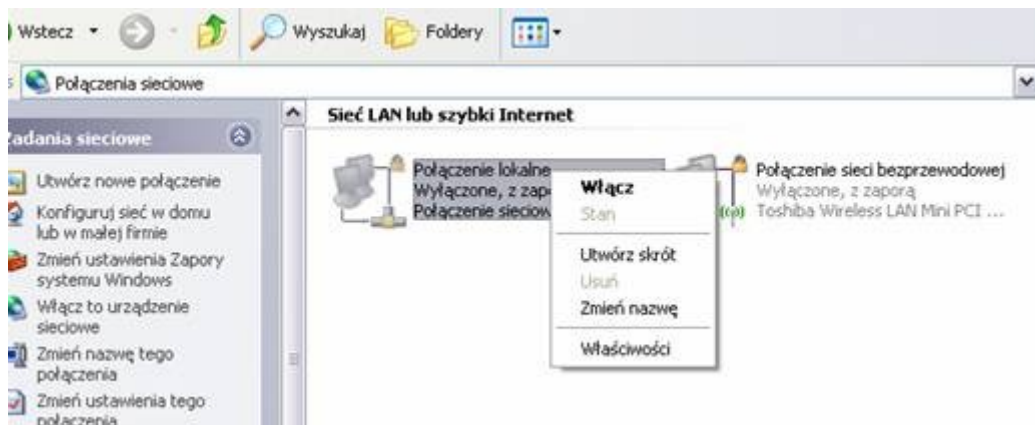
- wszystkie urządzenia zintegrowane na płycie głównej
- karty graficzne (sterowniki systemowe nie pozwalają na maksymalne wykorzystanie możliwości akceleratorów)
- inne karty (np. karty telewizyjne, itp.)
- pozostałe napędy i programy do ich obsługi
- dodatkowe kodeki, kompresory i dekompresory multimediów
- wszystkie inne programy, z których mamy zamiar korzystać
- dokonać aktywacji systemu, lub zmiany klucza systemu (jeśli posiadamy taką wersję)
- sformatować pozostałe partycje

Podłączenie komputera do sieci

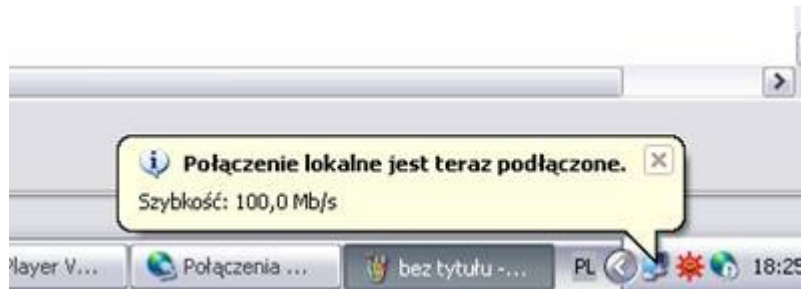
W większości przypadków dostęp do sieci lokalnych i Internetu jest realizowany poprzez kartę sieciową. Fizycznie jest to podłączenie zrobione za pomocą skrętki UTP zakończona wtykiem RJ45. Konfiguracja tego podłączenia polega na wyszukaniu w Panelu Sterowania ikony „Połączenia sieciowe„.



Następnie wybraniu połączenia które chcemy uaktywnić. W naszym przykładzie to „Połączenie lokalne”



O nawiązaniu połączenia zostaniemy poinformowani komunikatem.

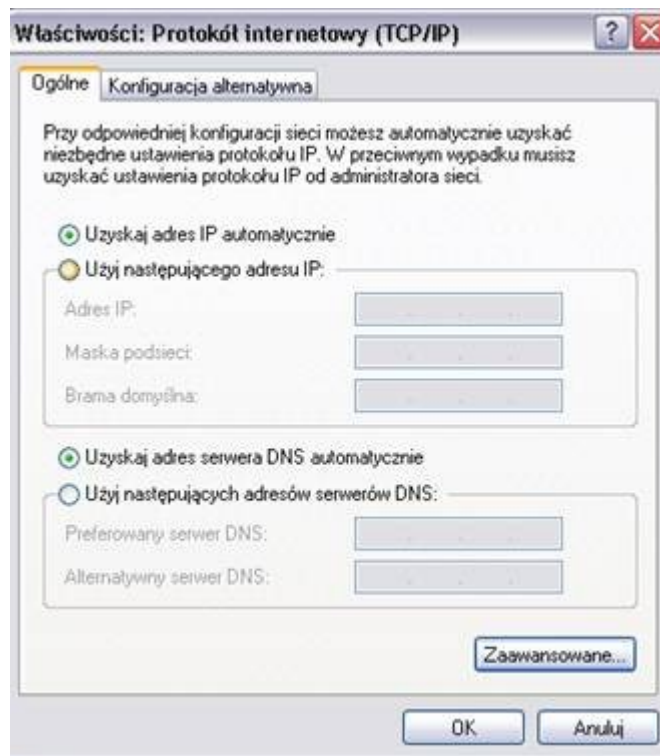


Jeżeli nasz dostawca internetowy wymaga abyśmy dodatkowo skonfigurowali połączenie to klikamy dwukrotnie na ikonę „Połączenie lokalne” następnie na zakładce „Ogólne” przycisk „Właściwości”

Następnie klikamy „Właściwości” dla Protokołu TCP/IP



W nowym okienku które pojawi się na ekranie będziecie w stanie wprowadzać potrzebne adresy IP oraz adres naszego serwera DNS. W przypadku laboratorium ustawienia domyślne (protokół DHCP) powinny być wystarczające.



Akceptujemy wszystko i włączamy raz jeszcze nasze połączenie.

Po wykonaniu tych wszystkich operacji mamy przygotowany komputer do pracy, lecz jeszcze nie zabezpieczony.

Zabezpieczanie naszego komputera

Nasz komputer, aby pracował długo i bez większych problemów podłączony do Internetu, należałoby:

- zwiększyć poziom bezpieczeństwa i ochronę przed nieporządanym dostępem do komputera
- stworzyć kopię zapasową systemu operacyjnego
- zabezpieczyć przed utratą niezbędnych danych.

Zagrożenia:

wirusy komputerowe to złośliwy kod programy. Najczęstsze działanie

polega na utrudnianiu pracy użytkownikowi na komputerze i jest to np:

- blokada dostępu do plików
- znikanie ikon
- dziwne reakcje systemu (swobodne poruszanie się kursora)

Bardziej wyrafinowanym działaniem jest fizyczne usuwanie danych. Wirusy komputerowe same nie są w stanie przenosić się z jednej maszyny do drugiej. Najczęściej drogą rozprzestrzeniania się ich jest poczta email (załączniki), strony WWW zawierające kod programu oraz fizyczne przenoszenie zainfekowanych danych z jednego komputera do innego.

robaki komputerowe to odmiana wirusów komputerowych, zdolna do samodzielnego rozprzestrzeniania się w sieci za pomocą wiadomości e-mail pod adresy wykradzione z książki adresowej programu pocztowego. Za pomocą luk w oprogramowaniu są wysyłane z naszego komputera w postaci spamu (niechcianej poczty). Jednym z takich robaków był Wblaster, który po podłączeniu zainfekowanego komputera do sieci Internet, wymuszał wyłączenie jednostki.

Sposobem walki w tego rodzaju programami jest:

- posiadanie zainstalowanego, dobrego programu antywirusowego z włączoną ochroną
- skanowanie plików kopiowanych do komputera
- aktualizowanie systemu operacyjnego

konie trojańskie są to głównie aplikacje udające pomocne narzędzia, wszelkiego rodzaju programy, wygaszacze ekranu, dodatki prezentujące na ekranie różne parametry (czas, pogoda itp.). W rzeczywistości dają po zainstalowaniu na naszym komputerze, twórcy oprogramowania:

- przejęcie kontroli nad naszym systemem
- kradzież danych
- możliwość niszczenia lub blokowania dostępu do zbiorów na dysku

Najczęstszym źródłem koni trojańskich są strony, witryny internetowe wyświetlające okienko pop-up (okienko reklamowe) po kliknięciu, którego instalowany jest złośliwy kod. Przykładem mogą być strony zawierające nielegalne oprogramowanie łamiące zabezpieczenia legalnych programów (crack, generatory kodów, itd.)

Kilka sposobów eliminacji koni trojańskich:

- dobry antywirus z aktualną bazą danych
- dokładne czytanie tego na co zamierzamy kliknąć i/lub zainstalować.
- włączone blokowanie okienek pop-up

Exploit jest to program lub kod źródłowy stworzony pod konkretną lukę systemu operacyjnego. Można go spotkać w kodach stron WWW. Jednym ze sposobów walki z nim to dbałość o aktualizację naszego oprogramowania, zastosowanie dobrej zapory ogniowej (Firewall'a), a ponadto programu antywirusowego z możliwością heurystycznych metod wyszukiwania zagrożenia.

Backdoor to program tworzący luki w oprogramowaniu komputera. Jest on rozsyłany za pomocą trojanów lub robaków internetowych. Zagrożenie, jakie ze sobą niesie to błąd w ochronie systemu, możliwość kontrolowania komputera przez nieautoryzowane osoby z zewnątrz.

Backdoor'a można usunąć programem antywirusowym. Natomiast pozostawioną lukę, jaką utworzył ten program identyfikuje się poprzez podpatrzenie, jakie porty w naszym połączeniu internetowym są otwarte, aktywne i przez jakie programy są aktualnie wykorzystywane. Jednym z takich prostych programów jest Active Ports.

Rootkit jest to program, który potrafi skutecznie ukrywać swoją obecność w systemie. Jeśli nie został jeszcze uaktywniony, może on być wykryty programem antywirusowym. Jednym z efektywnych sposobów jego wykrycia jest przeskanowanie dysku po podłączeniu go do innego „zdrowego” komputera lub z płytki uruchamialnej – LiveCD.

Spyware jest terminem opisującym oprogramowanie szpiegujące. To nie tylko cały program, także może być nim fragment kodu np. pliki cookies – wykorzystywane przez przeglądarki WWW – powiadamiające o naszych upodobaniach, preferencjach, krokach w Internecie (ulubionych, często odwiedzanych stronach), aktualnie wykonywanych operacjach w systemie firmy marketingowe. Mając taką pozyskaną informację, są one w stanie tak stworzyć i ukierunkować reklamy, aby mieć jak największą efektywność.

Najczęściej takie oprogramowanie można usuwać programem antyspyware np. popularnym Ad-Aware SE lub SpyBot S&D i innymi o podobnym działaniu.

Keylogger jest to program monitorujący użycie klawiatury. Rejestruje on używane klawisze. Zapisuje i wysyła tę informację w określone sobie miejsce w sieci Internet. Zagrożenie, jakie ze sobą niesie jest na tyle istotne, że nawet, jeśli strona w trakcie logowania się, wypełniania formularzy z ważnymi danymi jest w sesji szyfrowanej, nie mamy dostatecznej gwarancji bezpieczeństwa.

Jednym ze sposobów na ograniczenie tego typu niebezpieczeństwa jest stosowanie klawiatur ekranowych na stronie logowania, gdzie przy użyciu urządzenia wskazującego wprowadzamy istotne znaki.

Phishing to metoda wykradania poufnych danych użytkownika poprzez wprowadzenie go w błąd. Złodziej wysyła potencjalnej ofierze informację o potrzebnej aktualizacji danych osobowych, loginu i haseł. Nieświadomy użytkownik wprowadza to wszystko poprzez podany przez nadawcę link do spreparowanej strony.

Pharming to odmiana metody wyludzania poufnych danych. Różnica polega na tym, że użytkownik wpisując adres WWW interesującej go strony trafia na spreparowaną stronę złodzieja. Podmiana następuje w serwerze tłumaczącym nazwy na adresy IP (DNS).

Jednym z lepszych sposobów na uniknięcie takich kłopotów jakie niosą te dwie metody jest:

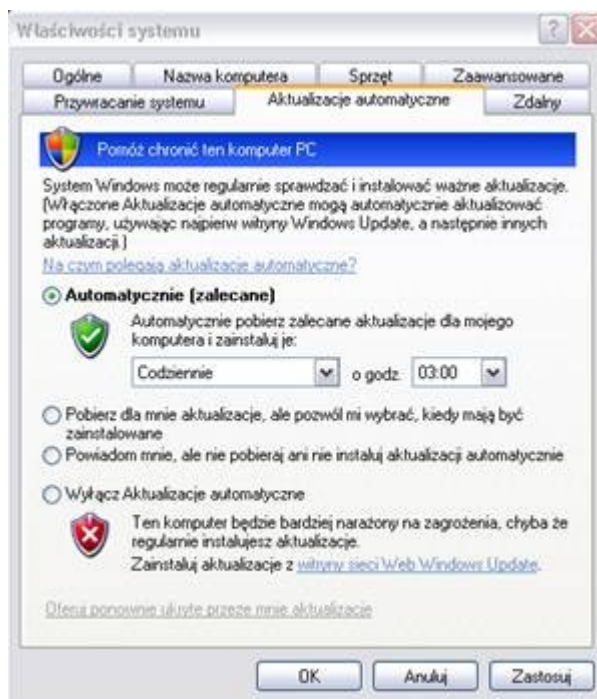
- być ostrożnym w obchodzeniu się z naszymi poufnymi danymi (nr kart itp.)
- ignorowanie i usuwanie e-maili nieznanego nam pochodzenia, nie reagowanie na treści w nich zawarte
- zainstalowanie nowoczesnych przeglądarek internetowych W celu lepszej ochrony przed opisanymi wcześniej zagrożeniami

należy przedsięwziąć niezbędne kroki. Poniżej została przedstawiona konfiguracja systemu, aby zabezpieczyć nasz komputer.

Aktualizacja systemu Windows XP

Jest to niezbędna funkcja systemu. Znajdziemy ją w:

Panel Sterowania System zakładka Aktualizacje automatyczne



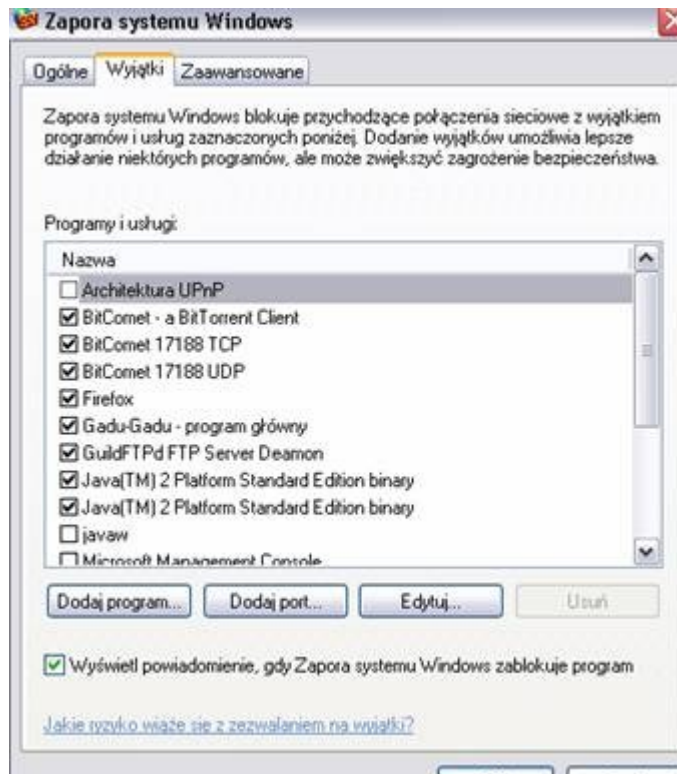
Zależnie od tego, kiedy chcemy dokonywać aktualizacji naszego systemu zaznaczamy jedną z trzech opcji. Aby aktualizacje przebiegały poprawnie, system musi zostać zarejestrowany w firmie Microsoft.

Uruchomienie i konfiguracja Zapory Systemowej Windows

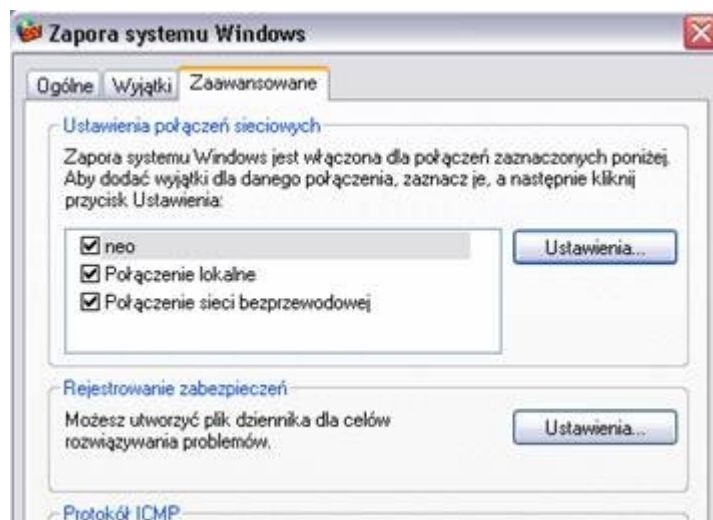
Zapora systemu Windows (dostępna w SP2). Znajdziemy ją w *Panel sterowania - Zapora*.



Następnie należy skonfigurować zaporę w odpowiedni sposób. Koniecznie musimy sprawdzić wyjątki na połączenia przychodzące do naszego komputera oraz przejrzeć, które są ustawione, a które chcemy ustawić. W naszym przypadku będziemy blokowali wszystkie połączenia przychodzące (te komputery nie będą pracowały jako serwery), natomiast pozwolimy na ruch wychodzący z naszego komputera. Takie ustawienia są domyślne dla systemu Windows.



Kolejno przedstawiono, które połączenia internetowe są przez zaporę obsługiwane – ukazuje to zakładka Zaawansowane.



Konfiguracja przeglądarki Internet Explorer

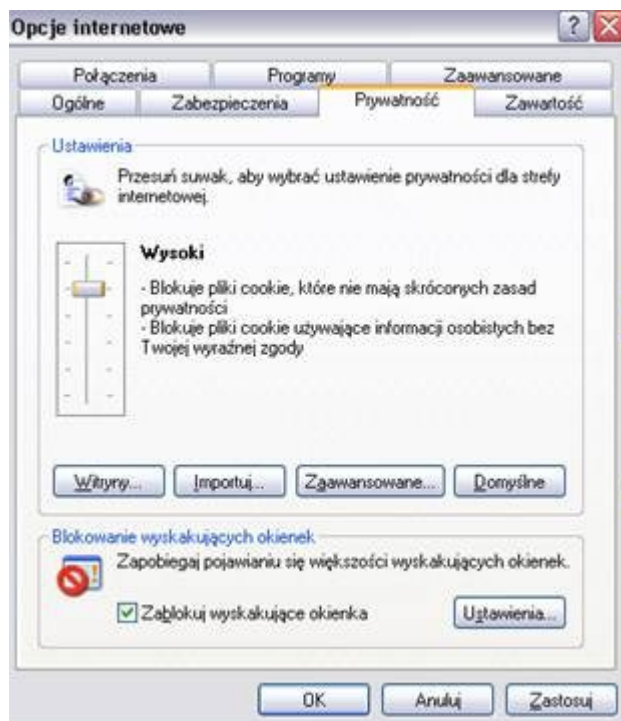
Ważnym elementem bezpiecznego przeglądania zasobów Internetu jest ustawienie przeglądarki. Możliwe jest wykorzystanie przeglądarki wbudowanej w system (Internet Explorer), my jednak na stałe będziemy korzystali ze zdecydowanie bezpieczniejszej przeglądarki – Firefox'a. By nie zostawiać dziury w systemie zabezpieczeń, na początek jednak skonfigurujemy też MS IE. Większość interesujących nas ustawień znajdziemy w menu *Narzędzia - Opcje Internetowe*

- zakładka *Ogólne*



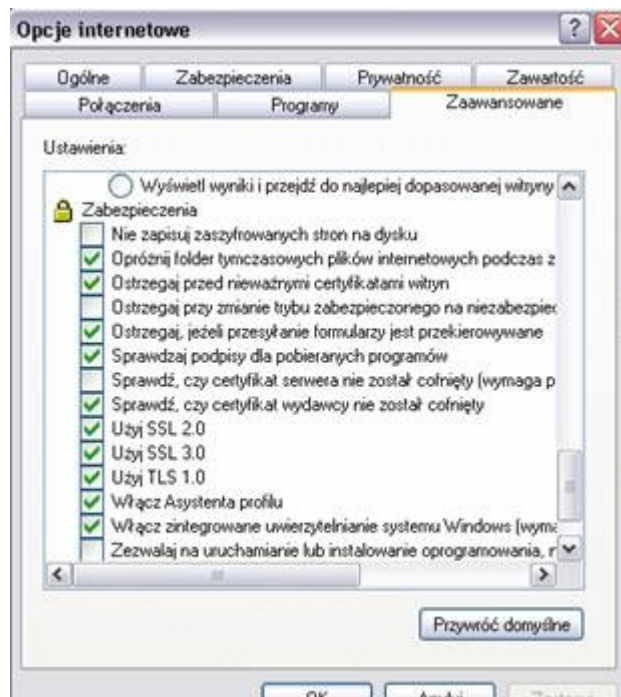
Można tutaj zarządzać danymi zbieranymi przez przeglądarkę podczas naszego surfowania po Internecie. Szczególnie przydatną funkcją jest czyszczenia historii przeglądanych stron i ręcznego usuwania zgromadzonych plików cookie

- zakładka *Prywatność*



W zakładce tej można ustawić opcję blokowania wyskakujących okienek pop-up jak i również sposób zachowywania się naszej przeglądarki poprzez suwak reprezentujący pięć stopni strefy bezpieczeństwa.

- zakładka *Zaawansowane*



Program antywirusowy

Następnym krokiem bezpiecznego komputera jest zainstalowanie dobrego programu antywirusowego, który zaktualizuje się poprzez połączenie do Internetu. Jest on w stanie wtedy sprawdzać i monitorować w sposób ciągły komputer. Tu mamy do wyboru bardzo wiele antywirusów. Czasem do komputera jest dodawany program Firmy Symantec. Są również inne kompletne zestawy Panda Software, Kaspersky, NOD32 itp. Odpowiedź, który program antywirusowy jest najlepszy, a który najskuteczniejszy nie jest prosta. Najlepiej sprawdzać ranking przed decyzją. My poprosimy Was o zainstalowanie programu wskazanego przez prowadzącego zajęcia, a w domowych zastosowaniach świetnie sprawdzają się darmowe wersje programów komercyjnych, jak np. BitDeffender, AVG, czy Amavis.

Instalacja programu antyspyware

Dobry program antyspyware'owy to taki, który ma możliwość aktualizowania bazy danych i tu przykładem może być Ad-Aware SE.



Posiada on funkcję pełnego skanowania naszego komputera w poszukiwaniu oprogramowania szpiegującego.



Zdarza się często tak, że jeden program typu freeware nie jest w stanie wykryć wszystkich programów szpiegujących w systemie. Dlatego też często instaluje się dwa konkurencyjne programy. Należy jednakże pamiętać o tym, aby stosować je na przemian, nie jednocześnie!

Dodatkowe oprogramowanie

Dobrym pomysłem na lepszą ochronę naszego komputera jest zainstalowanie jeszcze jednej przeglądarki internetowej. Na rynku jest wiele atrakcyjnych i sprawnych programów tego typu konkurujących z wbudowaną przeglądarką w Windows – Internet Explorer (IE). Ponadto programy spoza koncernu Microsoft oferują znacznie szersze możliwości konfiguracji o dobrze rozbudowanych mechanizmach wykrywania złośliwego oprogramowania umieszczanego na stronach internetowych. Na tych komputerach zainstalujemy przeglądarkę Mozilla Firefox. W tym celu pobieracie z internetu spod adresu:

<http://www.mozilla-europe.org/pl/firefox/>

wersję instalacyjną przeglądarki, a następnie instalujecie ją w standardowy sposób. Ustawiacie także tą przeglądarkę jako domyślną w systemie.

Poprosimy Was także o zainstalowanie programu Adobe Reader (przydatny w korzystaniu z tego dokumentu) oraz wybranego środowiska programistycznego (BCB lub Delphi w zależności od wybranego języka programowania).

Kopia zapasowa

Pierwszy dzień zajęć zakończymy stworzeniem kopii zapasowej świeżo zainstalowanego systemu, tak na wszelki wypadek ;)

Instalacja systemu Linux

Drugi dzień laboratorium rozpoczniemy od instalacji i konfiguracji systemu Linux jako stacji roboczej, oraz serwera małej sieci lokalnej. Wykorzystamy do tego celu dystrybucję Kubuntu lub Ubuntu – obie charakteryzują się wyjątkowo prostym procesem instalacji, łatwiejszym nawet niż Windows.

Ustawienia wstępne komputera

Ustawienia wstępne komputera są identyczne jak w przypadku instalacji Windows XP – również będziemy wykorzystywali płytę CD/DVD jako nośnik instalacyjny. Podstawowa różnica polega na działaniu instalatora. O ile instalator Windows jest specjalnym programem zastępującym system operacyjny, o tyle instalator Ubuntu / Kubuntu jest programem, który pracuje pod kontrolą systemu Linux. Dlatego też system wystartuje do wersji Live (uruchamianej z CD, lecz w pełni funkcjonalnej), i dopiero potem będziecie mieli możliwość uruchomienia instalatora i zdefiniowania podstawowych ustawień.

Partycjonowanie

Linux do poprawnej pracy wymaga istnienia na dysku co najmniej 2 partycji. Jedna z nich wykorzystywana jest jako pamięć wirtualna (SWAP), druga natomiast zawiera drzewo plików. Nasza instalacja będzie przeprowadzona przy wykorzystaniu 3 partycji, w układzie typowym dla stacji roboczych. Oprócz partycji SWAP oraz partycji głównej (root), jako niezależną partycję zainstalujemy również katalogi domowe użytkowników (/home). Rozmiar przeznaczony na każdą z nich zależy od wolnego miejsca na dysku, jednak ogólne zasady mówią, że:

- partycja SWAP powinna być ok 2 razy większa niż pamięć RAM komputera
- partycja główna (root) powinna mieć ok 5-10 GB
- reszta dysku jest przeznaczona albo na katalogi domowe (home) w przypadku stacji roboczych, albo na dane serwerów (var) w przypadku serwerów baz danych / www

Wstępna konfiguracja systemu:

Wszystkie zadania administracyjne w Linux-ach może wykonywać jedynie osoba o uprawnieniach administratora. W przeciwieństwie do Windows – nikt nie pracuje normalnie wykorzystując konto o takich prawach. W systemach pochodzących od Debiana, ograniczenia posunięto jeszcze dalej – nie można w ogóle logować się na konto administratora. Natomiast zawsze, jeśli to jest potrzebne – możemy uruchomić dany program jako administrator, służy do tego komenda

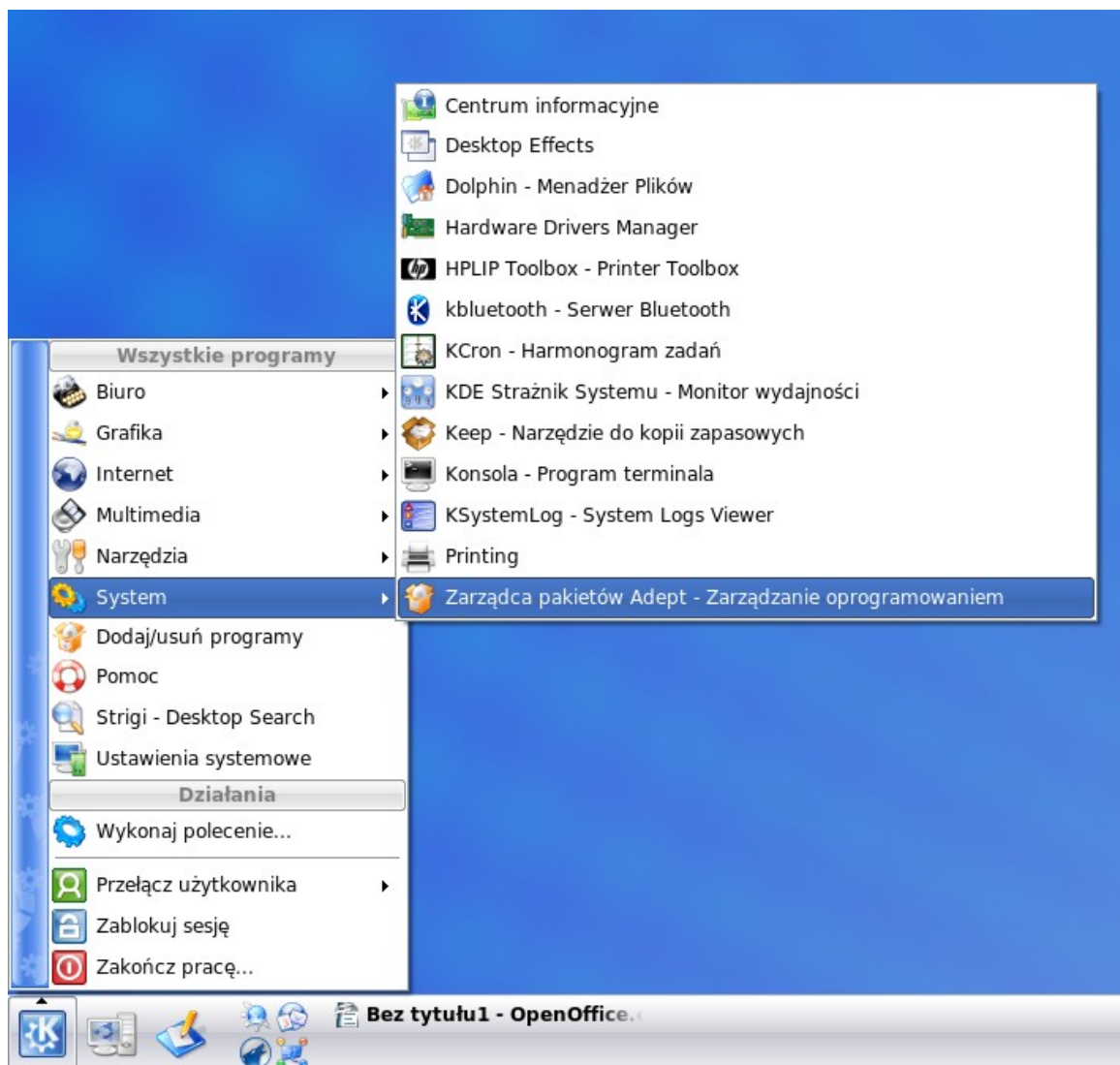
```
sudo <polecenie>
```

lub wywołanie (najczęściej automatyczne) programu kdesudo, który jest graficznym odpowiednikiem sudo.

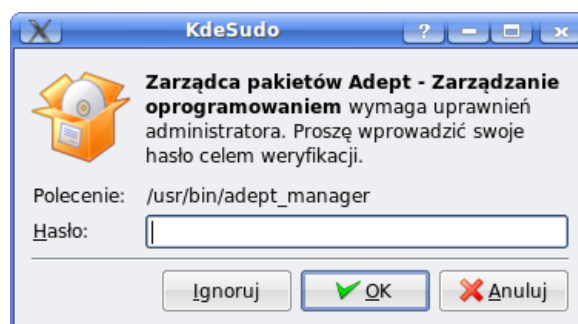
Pierwszym krokiem wykonywanym po zainstalowaniu jest uaktualnienie systemu. Można go dokonać wydając polecenie w konsoli:

```
sudo apt-get update && sudo apt-get upgrade
```

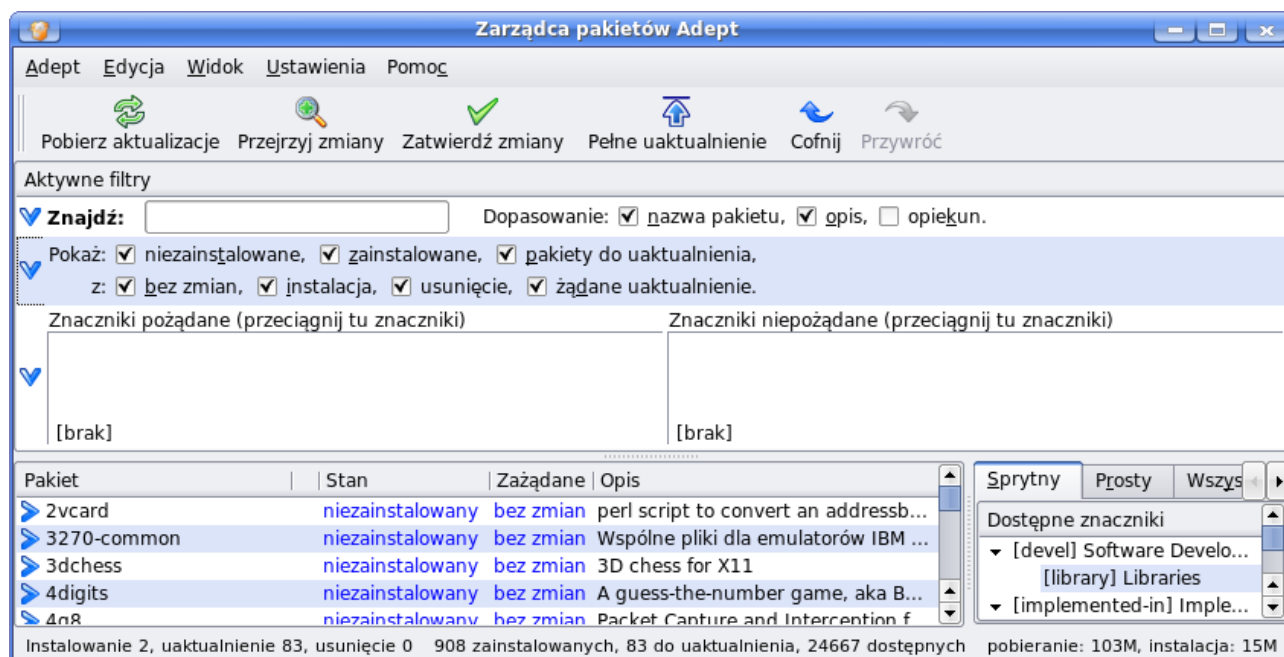
lub też skorzystać z programu Adept – który w Kubuntu pełni rolę zarządcy pakietów (w Ubuntu podobne zadanie pełni Synaptic). Wywołanie Adept jest możliwe poprzez pozycję System | Zarządca pakietów Adept z menu K:



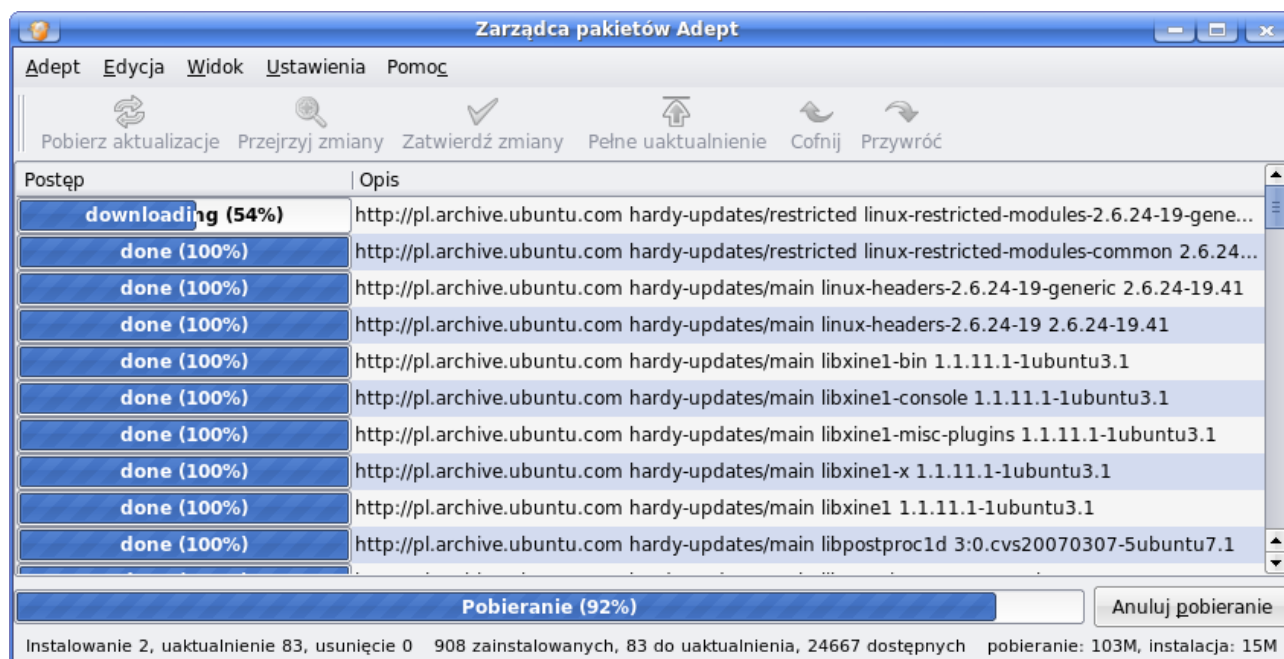
System poprosi Was o podanie hasła administratora (podobnie będzie reagował przy każdej operacji zmiany konfiguracji systemu, przy czym by nie męczyć zbytnio użytkownika, po pierwszym podaniu hasła zapamięta je na jakiś czas):



Podajemy hasło, i naszym oczom ukazuje się główny ekran pakietu Adept:



Dalsze postępowanie jest proste – wybieracie przycisk „Pełne uaktualnienie”, a następnie „Zatwierdź zmiany”. Linux w tym momencie przystąpi do pobierania uaktualnień z internetu, a następnie do ich instalacji:

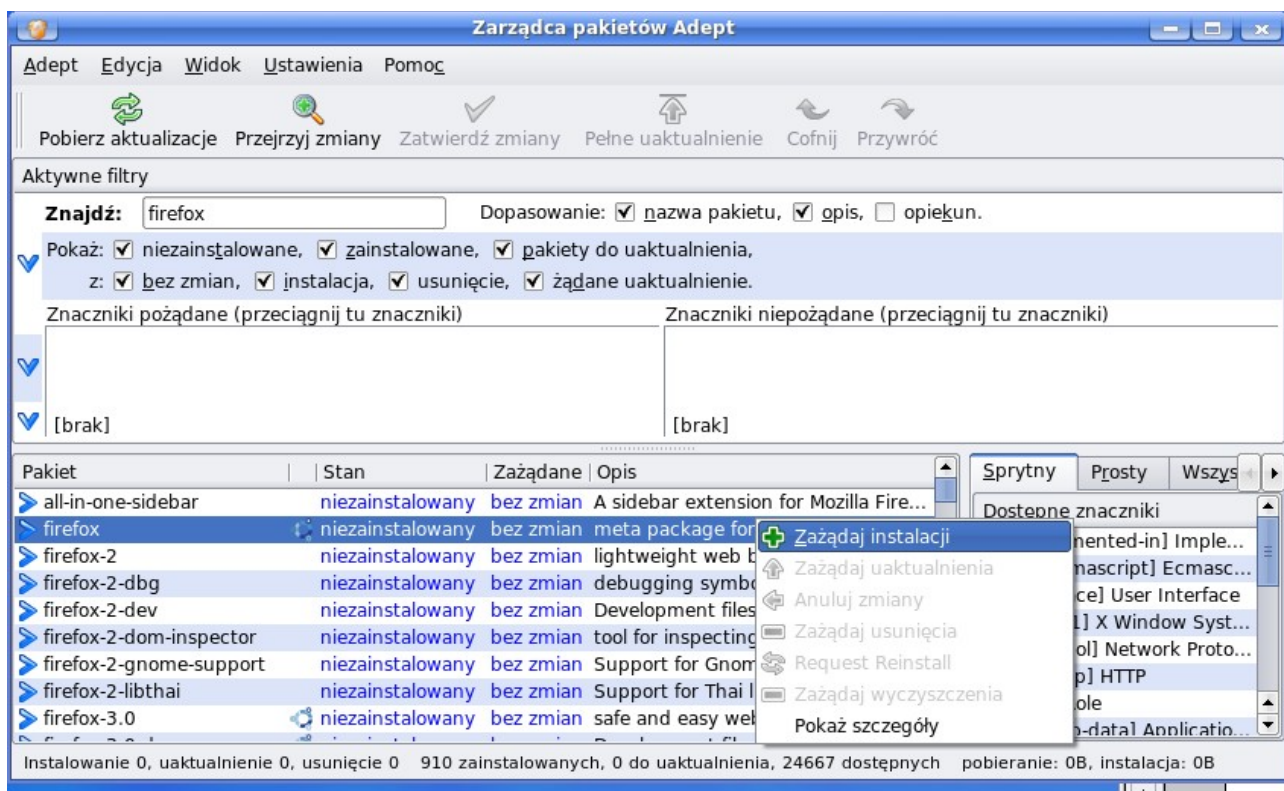


Instalacja dodatkowego oprogramowania

Zacznijmy od uzupełnienia standardowego oprogramowania o inną przeglądarkę internetową, czyli zainstalujemy Firefox-a. W tym celu w konsoli podajemy polecenie

```
sudo apt-get install firefox
```

lub w pole „Znajdź” wprowadzamy nazwę szukanego programu (firefox) a następnie wybieramy go na liście, klikamy prawym klawiszem myszy, i wybieramy opcję „Zażądaj instalacji”:



Potem znów „Zatwierdź zmiany” i czekamy aż firefox zainstaluje się na naszym komputerze.

W analogiczny sposób możecie zainstalować dowolny program dostępny w repozytoriach Ubuntu / Debiana.

Serwer plików sieci lokalnej

Pora przejść do instalacji serwera plików dla sieci lokalnej. W tym celu instalujemy pakiet „samba” w analogiczny sposób jak Firefox. Po zainstalowaniu uruchomi się on natychmiast jako demon (czyli dobry duszek ;)) systemowy. Domyślnie Samba nie będzie udostępniała żadnych zasobów z wyjątkiem ew. drukarek podpiętych do naszego komputera. Aby to zmienić, można skorzystać z któregoś z graficznych nakładek konfiguracyjnych (najlepszy jest chyba SWAT), lub też bezpośrednio edytować plik konfiguracyjny. Ponieważ pracujecie pod Linux-em, my proponujemy Wam tę drugą metodę.

Główny plik konfiguracyjny Samby jest w katalogu:

```
/etc/samba/
```

i nazywa się smb.conf

O ile nie korzystaliście wcześniej z konfiguratorów graficznych, plik ten zawiera dziesiątki komentarzy opisujących najpopularniejsze parametry. Każda linijka w pliku konfiguracyjnym ma określone znaczenie definiowane poprzez pierwszy jej znak. Jeśli tym znakiem jest # lub ; to mamy do czynienia z komentarzem – komentarze są ignorowane w trakcie czytania tego pliku przez demona. Linie z zawartością objętą nawiasami kwadratowymi to sekcje, pozostałe linie definiują parametry konfiguracyjne.

Przykładowy plik, który dostajecie po zainstalowaniu programu, zawiera tylko niewielką część najczęściej wykorzystywanych opcji. Opis wszystkich jest dostępny albo na stronie manual-a (polecenie `man smb.conf`), albo w internecie pod adresem

<http://www.samba.org>

polecamy też inne strony, dotyczące konfiguracji samby, np.
<http://blog.siebab.net/2007/05/samba-instalacja-konfiguracja.html>

(z tej strony pochodzi przykładowy plik konfiguracyjny zamieszczony niżej) oraz książkę „Using samba” (pdf w polskiej wersji językowej do pobrania z <http://iair.mchtr.pw.edu.pl/~pwnuk/download/samba.pdf>)

```
#####
# sekcja globalnej konfiguracji Samby
# (c)2000,2001 bs@vt.pl
#
[global]
comment = Polaczenie z venom ...
log file = /var/log/samba/%I.log
dont descend =
/dev,/proc,/root,/stand,/bin,/dist,/etc,/lkm,/mnt,/sbin,/sys,/usr

# opcje dla 10/100Mbit Half/Full Duplex
# takie ustawienie daje maksymalną szybkość w LAN
# w zależności od specyfiki konkretnej sieci, może wymagać modyfikacji
socket options = TCP_NODELAY SO_SNDBUF=16384 SO_RCVBUF=16384 IPTOS_LOWDELAY

# włączenie tych dwóch opcji zwiększa zwykle szybkość Samby o kilkanaście
procent
# choć z moich analiz wynika, że praca z bazami danych jest trochę szybsza
bez tego
read raw = yes
write raw = yes

# buforowanie katalogów
getwd cache = yes

# buforowanie zapisu plików zdecydowanie poprawia prędkość
# ale stwarza niebezpieczeństwo że Samba "nie zdąży" rzucić buforów na
dysk
# przy np. padzie zasilania (bez ups'a) plik taki będzie uszkodzony
# coś za coś, stosować z umiarem ;)
write cache size = 65536

# nadajemy Sambie nazwę w sieci windows
netbios name = venom

# chcemy mieć w miarę szczegółowe logi z dostępu do plików i zasobów
debug level = 2
debug timestamp = no
timestamp logs = True

# wielkość logów na peceta w KB, logi automatycznie przycinane przez Sambę
# czyli w rzeczywistości mamy zawsze po dwa pliki: oryginał i oryginał.bak
max log size = 5000

# chcemy aby Samba "słuchała" tylko na jednej z kilku naszych kart
sieciowych
bind interfaces only = True
interfaces = 10.0.0.1/255.255.255.0
hosts allow = localhost, 10.0.0.0/255.255.255.0

# tutaj konfigurujemy sposób obsługi drukowania
printing = bsd
printcap name = /etc/printcap
map archive = no
status = yes
public = no
read only = no
lpq cache time = 10

# tutaj ustawiamy opcje dotyczące konwersji nazw plików, wielkości liter
itp.
preserve case = yes
```

```

short preserve case = yes
strip dot = no
hide dot files = yes

# strona kodowa na pecetach
client code page = 852

# strona kodowa na uniksie
character set = iso8859-2

# tryb poziomu bezpieczeństwa zasobów
# (user=wymagane konto na uniksie oraz konto samby)
security = user
guest ok = no
browseable = yes

# domyślny tryb tworzenia plików -rw-----
create mode = 0700

# to odpowiada za superdostęp którego jednak nie chcemy :)
# admin users = root

# przydatne
unix realname = yes

# każdy dozwolony zapis do pliku zmienia timestamp pliku (jak w dos)
dos file times = yes

# ustawiamy grupę roboczą naszej sieci
workgroup = vtest

# zrzucamy połączenie po czasie 15minut w przypadku braku otwartych plików
# lub braku odpowiedzi z peceta
dead time = 15
keep alive = 15

# parametry ilości otwartych plików, zasobów itp.
mangled stack = 100
shared mem size = 1048576
max open files = 500

# chcemy aby Samba obsługiwała wyświetlanie wszystkich zasobów sieci, oraz
# udostępniała
# tzw roaming profiles (jak w NT)
domain master = yes
local master = yes
preferred master = yes

# ponieważ mamy tylko jedną podsieć, "cross subnet browsing"
# nie będzie nam potrzebny. Być może zrobimy drugą podsieć, zatem włączymy
# usługę WINS
wins support = yes
os level = 64

# niech nasza Samba działa "prawie" jak NT
nt smb support = yes
nt pipe support = yes
nt acl support = no

# Logowanie do domeny dla Windows 3.x, 95, 98,
# przechowywanie profili użytkowników na serwerze
# włączenie skryptów logowania mapujących np. dyski, drukarki itp.
domain logons = yes
logon script = startup.bat
logon path = \\%L%\%U

```

```

# chcemy żeby wszystkie pecety synchronizowały datę i czas zgodnie
# z naszym serwerem (jak w NetWare)
time server = True

# kolejność w jakiej Samba robi rozwiązywanie nazw netbiosowych pecetów
name resolve order = wins bcast hosts lmhosts

# nie chcemy, aby hasło windows'a = hasłu unixsa
# bowiem wymaga to specyficznego skonfigurowania procedury synchronizacji
# zależnej od konkretnego unixsa
unix password sync = false
update encrypted = no
passwd program = /usr/bin/passwd %u
passwd chat debug = false
passwd chat = *New*password* %n\n *Retype*new*password* %n\n
*updating*done*

# chcemy, żeby hasła były szyfrowane (jak w Windows 98, NT),
# Windows 95 wymaga przestawienia na taką pracę
# poprzez modyfikację rejestru. Odpowiednie pliki *.reg są dostępne w
# źródłach Samby.
# Tryb pracy z szyfrowanymi hasłami Samby pozwala na zmianę
# hasła sieciowego z poziomu "Panelu sterowania" w Windows.
encrypt passwords = yes
null passwords = false

# Komentarz widoczny w trybie szczegółów w "Otoczeniu sieci" Windows
server string = Serwer Venom

# Sekcje konfiguracji zasobów Samby

#####
[homes]
# ta sekcja mapuje unixowy katalog $HOME użytkownikowi
comment = Twój własny katalog

# przykładowo, prawa na katalogach domowych użytkowników /home
# powinny wyglądać tak:
# $>ls -l /home
# drwx-----  3 piotrek  piotrek          512 22 Sty  2000 piotrek

# prawa do plików i katalogów tylko dla właściciela
create mode = 0700
directory mode = 0700
public = no
writable = yes

# ścieżka do zasobu (czyli $HOME z /etc/passwd)
path = /home/%u
browseable = no

# zezwalamy na agresywne buforowanie plików przez Windows co
# daje znaczące zwiększenie szybkości Samby.
# Bezsensownym jest stosowanie tego na zasobach bazodanowych itp.
# "oplock" = "opportunistic lock"
oplocks = True
level2 oplocks = True

# przykładowo zabramy oplock'ów na plikach *.dbf i *.DBF
# veto oplock files = /*.DBF/*.dbf/

#####
[netlogon]
# ta sekcja udostępni zasób dla wszystkich, przy logowaniu do serwera
# w którym trzymamy globalny logonskrypt,
# pliki założeń Windows Policy (config.pol) - patrz dokumentacja Windows,

```

```

# a w szczególności program poledit.exe. Windows przy logowaniu nakłada
# parametry i ograniczenia pobierane z pliku config.pol na logującego się
# użytkownika. Modyfikowany jest rejestr tego użytkownika.
# prawa na katalogu powinny być takie:
# drwxr-xr-x    2 root    wheel                512 14 Sty  2000 netlogon

comment = Net Logon Service
path = /home/netlogon

case sensitive = no
create mode = 0755
directory mode = 0770
guest ok = yes

# nie potrzebujemy blokowania plików bo zasób jest tylko do odczytu
locking = no
writable = no
share modes = no

browseable = yes

# pozwalamy jednak na zapis do niego użytkownikom w uniksowej grupie inf,
# patrz plik /etc/group
write list = @inf

#####
[hpdj]
# tutaj udostępnimy drukarkę sieciową
# nazwa [hpdj] musi być identyczna jak w /etc/printcap

# tu wrzucane będą pliki tymczasowe wydruków, następnie kasowane
# po przesłaniu na drukarkę przez daemona lpd
path = /home/tmp
comment = HP Desk Jet 600
writable = yes
printable = yes
create mode = 0700
read only = yes

# ta drukarka jest tylko dla użytkowników uniksowej grupy pub
write list = @pub

# oraz wyłącznie z serwera i tych pecetów
hosts allow = 10.0.0.1 10.0.0.100 10.0.0.110

# tą komendą Samba będzie drukować
print command = /usr/bin/lpr -r -h -P %p %s

#####
[pub]
# Zrobimy zasób dostępny dla wszystkich z naszej sieci Windows,
# posiadających konto na serwerze
# prawa na tym katalogu powinny być takie:
# drwxrwx---    2 root    pub                  512 25 Sie 22:59 pub

path = /home/pub
volume = pub
comment = Katalog dla lokalnych
browseable = yes

# prawa muszą być także dla grupy, bowiem nikt z członków grupy
# nie mógłby nic zrobić z plikami innego członka grupy
create mode = 0770
directory mode = 0770

write list = @pub

```

```

oplocks = True
level2 oplocks = True

# dajemy dostęp do niego tylko z części sieci
hosts allow = 10.0.0.1/255.255.255.240

#####
[goscie]
# Zróbmy katalog dla innej grupy

path = /home/goscie
volume = goscie
comment = Katalog dla wszystkich
browseable = yes
create mode = 0770
directory mode = 0770
write list = @goscie
oplocks = True
level2 oplocks = True

#####
[bazy]
# Specjalna sekcja na potrzeby systemów bazodanowych, finansowo
# księgowych itp. Dostęp współdzielony bez oplock'ów

path = /home/bazy
volume = bazy
comment = Katalog baz danych
browseable = yes
create mode = 0770
directory mode = 0770
write list = @bazy

# zakaz stosowania agresywnego buforowania przez windows
oplocks = False
dos filetime resolution = True

#####
[cdrom]
# Czasem trzeba coś zainstalować na pecetach z udostępninego
# i podmontowanego cdromu na uniksie :)
# drwxr-xr-x  2 root  wheel          512 15 Kwi 17:45 cdrom

path = /cdrom
volume = cdrom
comment = Napęd CDROM
read only = yes
fake oplocks = yes
locking = no
writable = no
share modes = no

#####
[programy]
# a tu trzymamy różne programy dla pecetów
path = /home/programy
volume = programy
comment = Programy użytkowe i nietylko
#read only = yes
create mode = 0775
directory mode = 0775
#fake oplocks = yes
oplocks = True
level2 oplocks = True
#locking = yes
#writable = no

```



```
#share modes = no

# oczywiście prawo zapisu ma tylko uniksowa grupa programy
write list = @programy

# czytać pliki może uniksowa grupa pub i goscie
read list = @pub, @goscie
hosts allow = 10.0.0.0/255.255.255.0

#####
[www]
# użytkownicy naszej sieci wolą robić strony www lokalnie,
# na swoich komputerach, pracując z zamapowanego dysku serwera i
# strasznie nie lubią zabawy z użyciem ftp do wkopiowywania
# stron na serwer, tak więc Sambo! Do dzieła!
# prawa na tym katalogu powinny być takie:
# drwxr-xr-x  4 root  pub          512 27 Sie 09:23 www
# a wewnątrz katalogi użytkowników dostępne ze świata poprzez
# Apache Web Server (co wymaga odpowiedniej konfiguracji apacza)
# articles          40 root      wheel      lrwxr-xr-x
# ~books            37 root      wheel      lrwxr-xr-x
# ~faq              18 root      wheel      lrwxr-xr-x
# ~handbook         23 root      wheel      lrwxr-xr-x
# ~samba            28 root      wheel      lrwxr-xr-x
# ~sharedoc         20 root      wheel      lrwxr-xr-x
# /tom              1024 tom       nobody     drwxr-x---
# /www.pit.com.pl   512 mikek     nobody     drwxr-x---
# index.html        688 webmaster webmaster -rw-rw-r--
# ...
#
path = /home/www
volume = www
comment = Dla stron WWW
create mode = 0775
directory mode = 0775
write list = @pub
oplocks = false
level2 oplocks = false

##### KONIEC KONFIGURACJI #####
```

Pora wrócić do naszej konfiguracji. W każdej chwili możecie sprawdzić, jak działa Wasz serwer przez wybranie System (przycisk obok menu K) | Zdalne miejsca | Zasoby Samby. Otworzy Wam się wtedy okno menagera plików Dolphin w trybie przeglądania sieci, bardzo zbliżonym do otoczenia sieciowego systemu Windows.

Konfiguracja samby będzie się sprowadzała do edycji pliku smb.conf.

Uwaga: by można było go zapisać, edycja musi być wykonywana jako administrator. Czyli albo w konsoli wydajecie polecenie

```
sudo kwrite /etc/samba/smb.conf
```

albo przeglądacie dysk w poszukiwaniu pliku za pomocą Dolphin-a, i następnie klikacie na nim prawym przyciskiem myszy, i wybieracie: Akcje | Edytuj jako root

Pierwsze co zrobimy, to zmienimy domyślną nazwę grupy roboczej i komputera (grupa robocza niech się nazywa Lab{numer_laboratorium}, a komputer komp{numer_komputera}. Następnie udostępnijcie katalogi domowe użytkowników. Na początek wystarczy odkomentować (usunąć średniki na początku) następujące linijki:

```

;[homes]
;   comment = Home Directories
;   browseable = no

```

zmienić wartości po parametrze

```
workgroup =
```

(nazwa grupy roboczej lub domeny) oraz dopisać gdziekolwiek w sekcji global parametr

```
netbios name =
```

(nazwa komputera).

Po wprowadzeniu tych zmian, wydajecie polecenie

```
testparm
```

by sprawdzić, czy wprowadzone zmiany nie zawierają błędów, i następnie

```
sudo /etc/init.d/samba restart
```

Do wykonania został jeszcze jeden ważny krok – zdefiniowanie choć jednego użytkownika naszego serwera samby. By to zrobić, skorzystamy z polecenia smbpasswd. Pisząc w konsoli:

```
sudo smbpasswd -a janina
```

dodacie użytkownika o nazwie janina. Wy oczywiście janiny nie będziecie dodawali, dodajcie użytkownika o nazwie takiej samej jaką wybraliście dla siebie podczas instalacji systemu. Po pewnym czasie wasz komputer zacznie być widoczny w sieci pod nową nazwą. Niestety – nie będzie ciągle widoczny żaden z jego dysków. Katalogi domowe domyślnie są ukryte, i pojawiają się na liście zasobów dopiero po zalogowaniu się na danym komputerze. Dodajmy więc jeszcze katalog publiczny – do odczytu i zapisu przez każdego, udostępniany pod nazwą „publiczny”, fizycznie udostępniający katalog **/home/all**. Najpierw tworzymy ten katalog:

```
sudo mkdir /home/all
sudo chown janina:users /home/all
sudo chmod 770 /home/all
```

Następnie na końcu pliku **smb.conf** dodajemy dodatkową sekcję:

```
[publiczny]
path = /home/all
comment = Katalog publiczny
browseable = yes
read only = no
create mode = 0770
directory mode = 0770
write list = @users
```

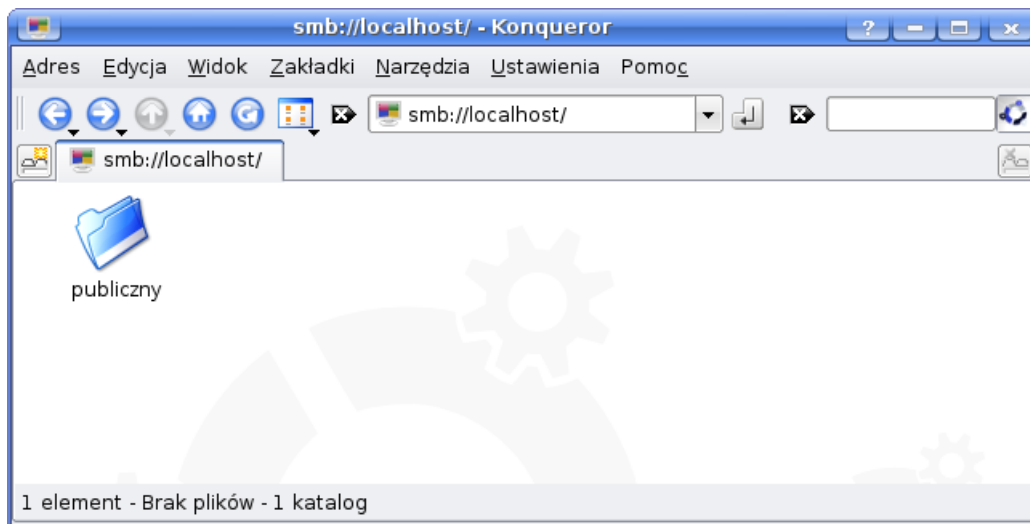
potem sprawdzamy plik konfiguracyjny i restartujemy sambę:

```
testparm
sudo /etc/init.d/samba restart
```

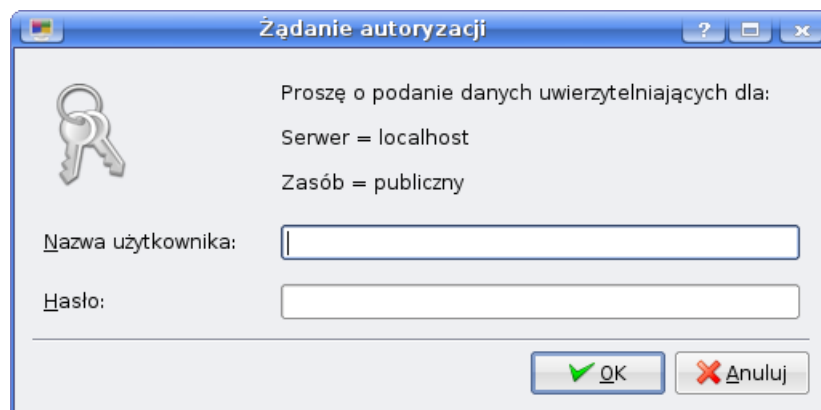
Niestety, zmiany które właśnie wprowadziliśmy, nie będą widoczne w otoczeniu sieciowym od razu. Będą od razu aktywne, lecz by były widoczne musi nastąpić synchronizacja maszyn udostępniających pliki, co w protokole smb zajmuje kilka – kilkanaście minut. Najprościej sprawdzić, czy odnieśliśmy sukces w zmianach konfiguracji korzystając z przeglądarki konqueror. Uruchamiamy ją (Menu K | Internet | Konqueror), i w pasku adresu podajemy:

```
smb://localhost
```

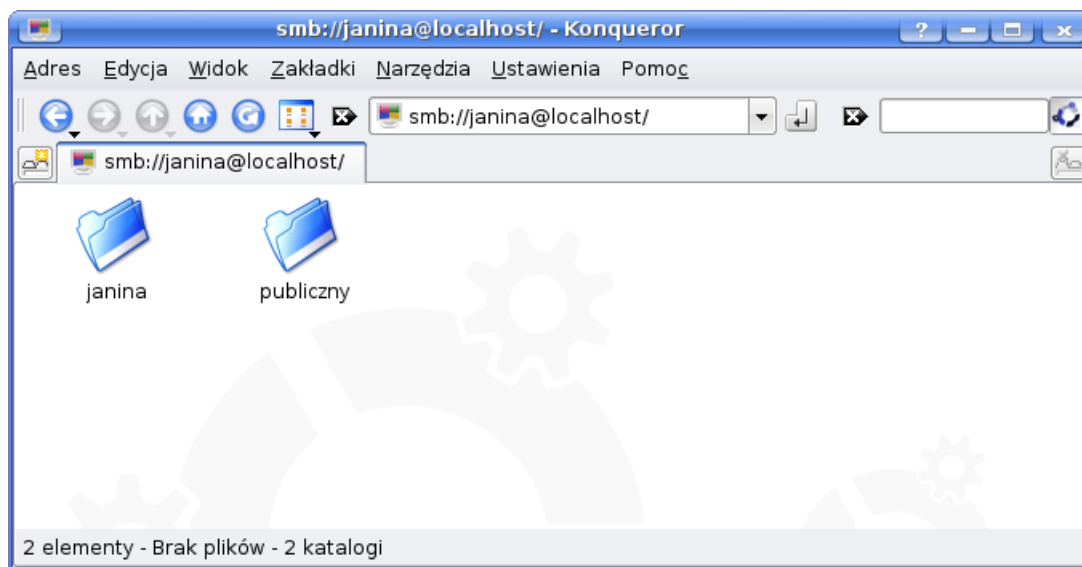
Powinniście otrzymać zbliżone okienko do poniższego:



teraz dwukrotne kliknięcie na **publiczny** wywoła okno autoryzacji



gdzie podajemy nasze dane (login i hasło samby), i możemy przetestować nasz udział publiczny. Zauważcie, że po powrocie do smb://localhost lista udostępnianych dysków zmieni się:



Po zalogowaniu widać już dyski, dla których parametr browseable jest nieaktywny (ma wartość **no**), czyli w moim przypadku – pojawiła się janina ;)

Kolejne zadanie wykonajcie już samodzielnie:

Udostępnijcie zawartość katalogu `/home/all_ro` jako dysk o nazwie `razem`, z możliwością zapisywania i kasowania plików przez każdego użytkownika z grupy `users` (podobnie jak nasz dysk publiczny), blokując jednak możliwość kasowania i zmian nie swoich plików (czyli jeśli **janina** utworzy na tym dysku plik o nazwie `dummy.txt`, to odczytać go może **zygmunt**, ale zapisać i skasować tylko **janina** – i vice versa). Dysk ma być niewidoczny dla użytkowników niezalogowanych.

Serwer www

Na komputerach w laboratorium zainstalujemy pełne środowisko tworzenia aplikacji www, w skrócie często określane jako LAMP (Linux, Apache, MySQL, PHP). Można oczywiście każdy z tych elementów instalować samodzielnie, można też wykorzystać piękno systemów zarządzania pakietami, które samoczynnie zainstaluje brakujące komponenty, i zainstalować pakiet `phpmyadmin`, który wymaga zarówno serwera apache, jak i języka php, co spowoduje że zostaną one zainstalowane w sposób automatyczny:

```
sudo apt-get install phpmyadmin
```

pozostaje jeszcze do zainstalowania baza danych:

```
sudo apt-get install mysql-server
```

i już wszystko powinno działać. Najprościej sprawdzić czy jest ok – uruchamiając przeglądarkę internetową i podając adres:

```
http://localhost
```

jeśli zobaczycie napis: `It works` – to znaczy że się udało ;) Dokładniejszy test będzie po uruchomieniu `phpmyadmin`-a, czyli:

```
http://localhost/phpmyadmin
```

jeśli zadziała, i zalogujecie się do bazy danych, to oznacza, że wszystkie komponenty LAMP działają prawidłowo.

Dokładna konfiguracja serwera Apache to (podobnie jak w przypadku Samby) temat na grubą książkę. Jednak tutaj domyślna konfiguracja w większości przypadków wystarczy. Serwer korzysta z plików konfiguracyjnych umieszczonych w `/etc/apache2`, przy czym w tym przypadku plików takich mamy wiele. Główny plik to **`apache2.conf`**, jednak on definiuje tylko podstawowe parametry. Lista udostępnianych katalogów www jest w plikach z podkatalogu **`sites-enabled`** (domyślnie mamy tam jedynie udostępniony katalog główny serwera `/var/www`), lista uruchomionych modułów w **`mods-enabled`**, konfiguracja dodatkowych aplikacji i modułów często jest też umieszczana w katalogu `conf.d`.

Jeśli zainstalujecie sobie dodatkowo dokumentację apache:

```
sudo apt-get install apache2-doc
```

uzyskacie dostęp do podręcznika konfiguracji apache pod adresem:

```
http://localhost/manual
```

Możecie go przejrzeć w skrócie, my w domyślnej konfiguracji włączymy jedynie możliwość udostępniania katalogów domowych użytkowników (co to oznacza, możecie przeczytać w dokumentacji apache: http://localhost/manual/en/howto/public_html.html). Nie będziemy jednak dopisywać dyrektyw, lecz wykorzystamy przygotowane pliki konfiguracyjne, które należy jedynie skopiować z **`mods-available`** do **`mods-enabled`**:

```
sudo cp /etc/apache2/mods-available/userdir.conf /etc/apache2/mods-enabled/userdir.conf
sudo cp /etc/apache2/mods-available/userdir.load /etc/apache2/mods-enabled/userdir.load
```

Na koniec zadanie dla Was – w oparciu o plik `/etc/apache2/conf.d/apache2-doc` przygotujcie plik konfiguracyjny, który będzie udostępniał zawartość katalogu `/home/all_html` pod aliasem

<http://localhost/all>

Uwaga: by zmiany w plikach konfiguracyjnych zaczęły działać, należy po każdej zmianie wydać polecenie

```
sudo /etc/init.d/apache2 restart
```