

Nazwa przedmiotu **Administracja i bezpieczeństwo systemów sieciowych**

Nazwa w języku angielskim **Administration and Security of Network Systems**

Język prowadzenia zajęć polski

Kierunek studiów Informatyka

Poziom studiów studia I stopnia inżynierskie

Jednostka prowadząca Katedra Mikroelektroniki i Technik Informatycznych, K-25

Kierownik i realizatorzy

dr inż. Mariusz Orlikowski	mariuszo@dmcs.pl
dr inż. Mariusz Orlikowski	mariuszo@dmcs.pl

Formy zajęć i liczba godzin w semestrze

Wyk.	Ćw.	Lab.	Proj.	Sem.	Inne	Suma godzin w semestrze
15	0	30	0	0	0	45

Efekty kształcenia

Umiejętność administrowania systemami sieciowymi na przykładzie systemu Unix (Linux). Umiejętność prawidłowej konfiguracji systemów operacyjnych. Znajomość zagadnień polityki bezpieczeństwa. Znajomość zagadnień bezpieczeństwa systemów sieciowych. Umiejętność konfiguracji systemu zabezpieczającego sieć lokalną.

Wymagania wstępne

Sieci komputerowe, Systemy operacyjne II

Organizacja przedmiotu i treści kształcenia

WYKŁAD

Bezpieczeństwo danych: definicja, planowanie i ocena ryzyka, polityka bezpieczeństwa danych w firmie, ochrona danych komputerowych, kopie zapasowe.
Bezpieczeństwo w systemach operacyjnych: typy ataków na systemy informatyczne, metody omijania zabezpieczeń, systemy regulacji dostępu i ochrony przed niepożądanym dostępem (użytkownicy, hasła, uprawnienia dostępu, zmiana uprawnień, superużytkownik), system plików na przykładzie ext2 i jego szczególne cechy w ujęciu bezpieczeństwa, systemy ochrony sieci lokalnych przed niepożądanym dostępem, ściana ogniowa, rodzaje ścian ogniowych i ich konfigurowanie.

ĆWICZENIA LABORATORYJNE

Instalacja i konfiguracja systemu Linux: konfiguracja podstawowych elementów systemu, uruchamianie systemu (omówienie mechanizmów uruchamiających system), uruchamianie demonów systemowych, uruchamianie i konfiguracja X-Window, kompilacja jądra, uwzględnianie poprawek.

Powłoka systemu: polecenia, strumienie, polecenia administracyjne.

Skrypty: przetwarzanie danych (polecenia awk, sed), zakładanie kont użytkowników.

Konfiguracja wybranych usług sieciowych: poczta, serwer i klient SSH, usługa logów systemowych, serwer i klient SMB, serwer DNS, serwer WWW, system haseł jednorazowych, tunelowanie i forwardowanie portów i inne. Konfiguracja bezpiecznych protokołów komunikacyjnych (SSH, SSL), klucze autoryzacyjne, certyfikaty.

Filtracja pakietów: konfiguracja systemu pełniącego funkcję firewall'a, wykrywanie udanych i nieudanych prób ataków.

Procesy: zarządzanie procesami, priorytety i ich zmiana.

Analiza systemu plików ze względu na niebezpieczne elementy (urządzenia, pliki SUID, GUID), bezpieczne podłączanie systemów plików.

Forma zaliczenia - sprawdzenia

Ocena końcowa przedmiotu składa się z testu zaliczającego i z oceny z laboratorium.

*osiągnięcia efektów
kształcenia*

*Literatura
podstawowa*

*Literatura
uzupełniająca*

1. Kirch O., Dawson T.: LINUX – Podręcznik administratora sieci. O'Reilly 2000.
2. Dudek A.: Nie tylko wirusy - hacking, cracking, bezpieczeństwo internetu. Wydawnictwo Helion 2004
3. Kifner T.: Polityka bezpieczeństwa i ochrony informacji. Wydawnictwo Helion 1999

*Przeciętne
obciążenie studenta
pracą własną*

15

*Całkowite obciążenie
studenta pracą*

60

Uwagi

Uwagi

Aktualizacja

2008-12-01