Bezpieczeństwo Sieci Komputerowych

dr inż. Marcin Markowski

Katedra Systemów i Sieci Komputerowych

Bezpieczeństwo Sieci Komputerowych

- Forma zaliczenia:
  zaliczenie - kolokwium
- Warunek konieczny:
  zaliczenie laboratorium
- Materiały do kursu:
  eportal.pwr.edu.pl
  klucz: *podany na laboratorium*

wtP_0815 ptP_0730 ptP_1015

CELE PRZEDMIOTU

- C1 Nabycie wiedzy z zakresu zagrożeń i podatności sieci komputerowych oraz mechanizmów ochronnych, w tym mechanizmów kryptograficznych
- C2 Nabycie umiejętności testowania bezpieczeństwa systemu informatycznego oraz konfiguracji mechanizmów zabezpieczających
- C3 Zrozumienie idei standaryzacji w dziedzinie bezpieczeństwa, świadomość aspektów prawnych i społecznych bezpieczeństwa informacji

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy:

- PEK_W01 Zna i rozumie typowe zagrożenia oraz podatności współczesnych systemów teleinformatycznych
- PEK_W02 Posiada wiedzę w zakresie środków i metod ochrony systemów, w tym mechanizmów kryptograficznych
- PEK_W03 Posiada wiedzę z zakresu metodyki przeprowadzania analizy ryzyka i audytu teleinformatycznego, potrafi wymienić i opisać standardy normujące ocenę bezpieczeństwa teleinformatycznego

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu umiejętności:

- PEK_U01 Potrafi zaprojektować i przeprowadzić testy bezpieczeństwa sieci komputerowej oraz przeanalizować wyniki testów i wyciągać wnioski
- PEK_U02 Potrafi korzystać z narzędzi kryptograficznych, szyfrować i deszyfrować, składać i weryfikować podpisy cyfrowe
- PEK_U03 Potrafi konfigurować i zarządzać mechanizmami bezpieczeństwa i bezpiecznymi usługami sieciowymi

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu kompetencji społecznych:

- PEK_K01 Rozumie ideę normalizacji i certyfikacji, zna i rozumie aspekty prawne i społeczne bezpieczeństwa informacji

Bezpieczeństwo Sieci Komputerowych

- Zaliczenie wykładu - kolokwium
- Ocena kolokwium: od 50%(3), 60(3.5), 70(4), 80(4.5), 90(5)
- Ocena końcowa z kursu:

  0,5 * Ocena_kolokwium + 0,5 * Ocena_lab

  Obie oceny muszą być pozytywne

Wykład – sprawy organizacyjne

- 7 * 90 min + 45 min (kolokwium)
- Słownictwo angielskie
- Pytania testowe pod koniec wykładu
- Urządzenia elektroniczne i Internet
- Artykuły spożywcze
- Kurtki, płaszcze

Program wykładu

- Zagrożenia i podatności
- Kryptografia, podpis cyfrowy
- Certyfikaty i infrastruktura klucza publicznego
- Uwierzytelnianie
- Bezpieczeństwo usług sieciowych
- Wirtualne sieci prywatne
- Filtrowanie i inspekcja ruchu sieciowego
- Standaryzacja i aspekty prawne

Literatura

- Stallings W., 'Kryptografia i bezpieczeństwo sieci komputerowych : matematyka szyfrów i techniki kryptologii', wyd. Helion, Gliwice, 2012
- Cole E., Krutz R., Conley J., 'Bezpieczeństwo sieci: biblia', wyd. Helion, Gliwice, 2005
- Dostálek L., 'Bezpieczeństwo protokołu TCP/IP: kompletny przewodnik', Wydawnictwo Naukowe PWN, Warszawa, 2006.
- Krzysztof Liderman, 'Analiza ryzyka i ochrona informacji w systemach komputerowych', Wydawnictwo Naukowe PWN: Mikom, Warszawa, 2008

Literatura

- Fry C., Nystrom M., 'Monitoring i bezpieczeństwo sieci', wyd. Helion, Gliwice, 2010
- Polaczek T., 'Audyt bezpieczeństwa informacji w praktyce: praktyczny przewodnik po zagadnieniach ochrony informacji', wyd. Helion, Gliwice, 2006
- Serafin, M., 'Sieci VPN: zdalna praca i bezpieczeństwo danych', wyd. Helion, Gliwice, 2010
- Stallings W., 'Ochrona danych w sieci i intersieci', WNT, Warszawa, 1997

Program laboratorium

1. Zagrożenia i podatności sieci komputerowych
2. Kryptografia
3. Bezpieczne usługi sieciowe, VPN
4. Zapory ogniowe, filtrowanie ruchu
5. Bezpieczeństwo infrastruktury sieciowej