KARTA KURSU

Nazwa	**Bezpieczeństwo systemów serwerowych**
Nazwa w j. ang.	Server security

Koordynator	mgr Alfred Budziak	Zespół dydaktyczny
		mgr Alfred Budziak
Punktacja ECTS*	st. stacjonarne: 2 st. niestacjonarne: 2	

Opis kursu (cele kształcenia)

Celem kursu jest zapoznanie studentów z wybranymi technikami zabezpieczania systemów serwerowych. Kurs prowadzony jest w języku polskim.

Warunki wstępne

Wiedza	Funkcjonowanie TCP/IP v4
Umiejętności	Umiejętność pracy na poziomie użytkownika z dowolnym systemem operacyjnym. Umiejętność pracy w powłoce unixowej/unixopodobnej lub w cmd (lub PowerCli) Windows (będzie wymagane zapoznanie się z polecaniami shella unixowego PRZED zajęciami)
Kursy	Zaawansowane technologie sieciowe

Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Wiedza	W01: Podstawowa „higiena” pracy z systemem W02: Narzędzia zabezpieczania systemu, testowanie bezpieczeństwa, DMZ i serwer bastionowy. W03: Detekcja intruzów w systemie.	K_W13 K_W13, K_W11 K_W13

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	U01: Konfiguracja podstawowych czynności codziennego utrzymywania systemu związanych z bezpieczeństwem. U02: Analiza ruchu input/output/forward na interfejsach serwera, produkcja skryptu konfigurującego ścianę ogniową U03: Konfiguracja oraz stosowanie narzędzi zabezpieczających i testujących system	K_U07 K_U05 K_U07

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	K01 – Potrafi docenić wagę bezpieczeństwa w świecie współczesnej technologii K02- Rozumie wagę współpracy między wieloma jednostkami/administratorami starającymi się konfigurować/implementować bezpieczeństwo.	K_K06 K_K07,K_K02

Studia stacjonarne

Organizacja													
Forma zajęć	Wykład (W)	Ćwiczenia w grupach											
		A		K		L		S		P		E	
Liczba godzin						30							

Studia niestacjonarne

Organizacja													
Forma zajęć	Wykład (W)	Ćwiczenia w grupach											
		A		K		L		S		P		E	
Liczba godzin						20							

Opis metod prowadzenia zajęć

Przedmiot prowadzony metodą laboratoryjną.
Studenci konfigurują różne rozwiązania na przydzielonych im „własnych” VPS (virtual private server) lub układach VPS-ów . Laboratoria będą wykonywane zarówno jednoosobowo jak i w grupach. Do podstawowych zadań studenta będzie należało poprawne wyszukanie dokumentacji i opisu konfigurowanych rozwiązań.

Formy sprawdzania efektów kształcenia

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01					x								
W02					x								
W03					x								
U01					x								
U02					x								
U03					x								
K01					x								
K02					x								
...													

Kryteria oceny	Zaliczenie student uzyskuje na podstawie wykonywanych na laboratoriach konfiguracji. Ocena zależy od jakości i zaawansowania przedstawionych rozwiązań.

Uwagi	Przedmiot niezwykle trudny do oceny ze względu na różne zaawansowanie studentów. Spodziewać się należy zarówno administratorów systemów operacyjnych jak i osób mało zaawansowanych w dziedzinie bezpieczeństwa systemów operacyjnych. Aby dobrze wykorzystać czas prowadzący powinien zindywidualizować poziom zaawansowania zadawanych konfiguracji w zależności od początkowych umiejętności studenta. Prowadzący może dowolnie wybierać narzędzia z jakich skorzysta w ramach zaplanowanych treści merytorycznych

Treści merytoryczne (wykaz tematów)

- „Utrzymywanie" codzienne serwera
- Bezpieczeństwo wybranych usług.
- Zarządzanie ruchem pakietów przez serwer, „manglowanie" pakietów
- ściany ogniowe
- VPN
- nakładki bezpieczeństwa na kernel
- hosty bastionowe
- DMZ
- IDS-y , bazy integralności
- skanery bezpieczeństwa, testowanie.

Wykaz literatury podstawowej

M.D. Bauer, „Linux , Servery , Bezpieczeństwo" , Helion 2005
M. Serafin Sieci VPN : zdalna praca i bezpieczeństwo danych, Helion 2008
T. J. Klevinsky, Hack I.T. : testy bezpieczeństwa danych , Helion 2003
Uwaga: Ze względu na dynamicznie zmieniające się metody pracy w tej dziedzinie oraz powszechną praktykę administratorów systemów operacyjnych literaturą do przedmiotu będzie przede wszystkim dokumentacja techniczna i poradniki „how-to" .

Wykaz literatury uzupełniającej

D.J. Barret, „Linux , bezpieczeństwo, receptury", Helion 2003
W. R. Cheswick," Firewalle i bezpieczeństwo w sieci". Helion, 2003
M. Serafin „Sieci VPN wydanie drugie", e-book, Helion 2013
M. Rush „Bezpieczeństwo sieci w Linuksie. Wykrywanie ataków i obrona przed nimi za pomocą iptables, psad i fwsnort", Helion 2008

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia stacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	
	Konwersatorium (ćwiczenia, laboratorium itd.)	30
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	5
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	
	Przygotowanie do egzaminu/zaliczenia	10
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia niestacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	
	Konwersatorium (ćwiczenia, laboratorium itd.)	20
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	10
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	
	Przygotowanie do egzaminu/zaliczenia	15
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2