

KARTA PRZEDMIOTU

A. Informacje ogólne

Wypełnia Zespół Kierunku	Nazwa modułu (bloku przedmiotów): Blok przedmiotów wybieralnych				Kod modułu: M23		
	Nazwa przedmiotu: Przedmiot dyplomowy wybieralny Administracja systemem LINUX II				Kod przedmiotu:		
	Nazwa jednostki prowadzącej przedmiot / moduł: INSTYTUT INFORMATYKI STOSOWANEJ im. Krzysztofa Brzeskiego						
	Nazwa kierunku: INFORMATYKA			Poziom kształcenia: pierwszy			
	Forma studiów: niestacjonarne		Profil kształcenia: praktyczny		Specjalność: Projektowanie baz danych i oprogramowanie użytkowe		
	Rok / semestr: 4/8		Status przedmiotu / modułu: obowiązkowy			Język przedmiotu / modułu: polski	
	Forma zajęć	wykład	ćwiczenia	laboratorium	projekt	seminarium	inne (wpisać jakie)
	Wymiar zajęć	15		15			
Cel przedmiotu / modułu		Wyposażenia studenta w praktyczną wiedzę umożliwiającą bezpieczne korzystanie z systemu operacyjnego Linux w charakterze stacji roboczej i serwera w sieci Internet. Rozszerzenie wiedzy z przedmiotu „Administracja systemem Linux I”.					
Wymagania wstępne		Znajomość zagadnień teoretycznych z zakresu działania sieci komputerowych oraz podstawy obsługi systemu Linux. Biegłe na poziomie użytkownika, w zakresie podstawowym na poziomie administratora.					
EFEKTY KSZTAŁCENIA							
Lp.	Opis efektu kształcenia					Odniesienie do efektów dla kierunku	
	Wiedza – student:						
01	Zna rodzaje zagrożeń występujących w sieciach komputerowych i Internecie.					K_W05, K_W08, K_W16 K_W17	
02	Wie jak chronić systemy, sieci i dane przed różnymi zagrożeniami.					K_W04	
03	Zna narzędzia zapewniające poufność i integralność danych.					K_W08, K_W12	
	Umiejętności – student:						
04	Potrafi skonfigurować zaporę sieciową w systemie Linux.					K_U05, K_U10, K_U13	
05	Wykorzystuje szyfrowanie asymetryczne do ochrony plików, katalogów, poczty elektronicznej. Zarządza kluczami. Wykorzystuje podpis cyfrowy.					K_U05, K_U10	
06	Bezpiecznie loguje się do systemu, monitoruje stan jego bezpieczeństwa i korzysta z niego z sieci zewnętrznej.					K_U05, K_U06, K_U10, K_U14, K_U22	
07	Generuje certyfikaty cyfrowe i wykorzystuje w bezpiecznej komunikacji WWW i FTP.					K_U05, K_U10	
	Kompetencje społeczne – student:						
08	Przestrzega etyki zawodowej, w tym poszanowania praw autorskich.					K_K03	
09	Chroni dane osobowe i firmowe.					K_K03	

Metody weryfikacji efektów kształcenia		Lp. efektu kształcenia
Kolokwium zaliczeniowe z teorii, terminów i poleceń.		01-03
Wykonanie zadanej konfiguracji na maszynie wirtualnej..		04-09
NAKŁAD PRACY STUDENTA		
Rodzaj działań/zajęć	Liczba godzin	
	ogółem	w tym zajęcia powiązane z praktycznym przygotowaniem zawodowym
Udział w wykładach	15	13
Samodzielne studiowanie tematyki wykładów	20	18
Udział w ćwiczeniach audytoryjnych i laboratoryjnych*	15	15
Samodzielne przygotowywanie się do ćwiczeń*	45	45
Przygotowanie projektu / eseju / itp. *		
Przygotowanie się do egzaminu / zaliczenia		
Udział w konsultacjach	5	
Inne	2	
ŁĄCZNY nakład pracy studenta w godz.	102	91
Liczba punktów ECTS za przedmiot	4 ECTS	
Liczba p. ECTS związana z zajęciami praktycznymi*	3,6 ECTS	
Liczba p. ECTS za zajęciami wymagające bezpośredniego udziału nauczycieli akademickich	37 1,5 ECTS	

B. Informacje szczegółowe

Wypełnia Zespół Kierunku	Nazwa modułu (bloku przedmiotów): Blok przedmiotów wybieralnych					Kod modułu: M23	
	Nazwa przedmiotu: Przedmiot wybieralny II Administracja systemem LINUX II					Kod przedmiotu:	
	Nazwa jednostki prowadzącej przedmiot / moduł: INSTYTUT INFORMATYKI STOSOWANEJ im. Krzysztofa Brzeskiego						
	Nazwa kierunku: INFORMATYKA			Poziom kształcenia: pierwszy			
	Forma studiów: niestacjonarne		Profil kształcenia: praktyczny		Specjalność: Administracja systemów i sieci komputerowych		
	Rok / semestr: 4/7		Status przedmiotu /modułu: obowiązkowy			Język przedmiotu / modułu: polski	
	Forma zajęć	wykład	ćwiczenia	laboratorium	projekt	seminarium	inne (wpisać jakie)
	Wymiar zajęć	15		15			
Koordynator przedmiotu / modułu		mgr inż. Mariusz Bagiński					
Prowadzący zajęcia		mgr inż. Mariusz Bagiński					
TREŚCI PROGRAMOWE							
Wykład							
<ol style="list-style-type: none"> 1. AppArmor, TCP Wrapper, arpwatch, chroot. 2. Narzędzia kopii zapasowych. 3. Firewall w systemie Linux. Strefa DMZ. 4. Funkcje skrótu: MD5 i SHA1. 5. Szyfrowanie symetryczne i niesymetryczne. GPG. 6. Certyfikaty cyfrowe. Podpis elektroniczny. 7. Ochrona poczty elektronicznej na serwerze i stacji roboczej. 8. OpenSSL. Certyfikaty w usługach: HTTPS, FTPS. 9. SSH, SFTP, certyfikaty w SSH. Tunele SSH. 10. Bezpieczne używanie tradycyjnych i rozszerzonych praw dostępu. 11. Oprogramowanie antywirusowe na serwerze i stacji roboczej Linux. 12. Logi systemowe - Syslog. Analiza logów. Rotacja logów. 13. Automatyczna analiza logów z użyciem pakietu oprogramowania OSSEC. (Trend Micro). 14. Systemy IDS/IPS. Implementacja systemu IPS z użyciem OSSEC i SNORT. 							
W tym treści powiązane z praktycznym przygotowaniem zawodowym: [90%]							
Laboratorium							
<ol style="list-style-type: none"> 1. Konfiguracja podstawowego bezpieczeństwa systemu. 2. Tworzenie kopii zapasowych w systemie Linux. 3. Konfiguracja zapory sieciowej – IPTABLES. 4. Obliczanie funkcji skrótu: sum, md5sum, XCSC, sha1sum. 							

5. Tworzenie certyfikatów SSL.
6. Uruchamianie usług HTTPS i FTPS.
7. GPG (GNU Privacy Guard) – szyfrowanie plików i katalogów, podpis cyfrowy.
8. GPG (GNU Privacy Guard) - szyfrowanie poczty elektronicznej, podpis cyfrowy poczty.
9. Ochrona poczty elektronicznej: POP3S, IMAPS, spam, antywirusy. Konfiguracja klienta w systemie Linux.
10. Szyfrowanie plików i partycji systemowych z użyciem narzędzia TrueCrypt.
11. Zarządzanie usługą SSH i SFTP, logowanie z użyciem certyfikatów.
12. Aplikacje: Nmap, Nessus, Wireshark, tcpdump i inne.
13. Bezpieczna manipulacja tradycyjnymi i rozszerzonymi listami kontroli dostępu (współdzielenie plików i katalogów, pliki systemowe, inne prawa dostępu).
14. Analiza logów systemowych („ręczna” i automatyczna – OSSEC).
15. Implementacja systemu IPS z użyciem SNORT i OSSEC.

W tym treści powiązane z praktycznym przygotowaniem zawodowym: [100%]

Literatura podstawowa	<ol style="list-style-type: none"> 1. „Linux – bezpieczeństwo. Receptury”, autor: D.J. Barrett i inni, Helion 2003. 2. „Bezpieczeństwo sieci w Linuksie. Wykrywanie ataków i obrona przed nimi za pomocą iptables, psad, fwsnort”, autor: Michale Rash, Helion 2008. 3. Strony podręcznika systemowego: man, info.
Literatura uzupełniająca	Materiały LPI. Źródła internetowe.
Metody kształcenia	Wprowadzenie, prezentacje, video, wykonywanie zadanych konfiguracji na maszynach wirtualnych.
Forma i warunki zaliczenia	Egzamin z teorii, pojęć i odpowiednich poleceń systemu Linux (wykład), wykonanie zadania na maszynie wirtualnej (lab.), odpowiednie wagi: 50% wykład, 50% lab.