

KARTA KURSU

Nazwa	Bezpieczeństwo sieci komputerowych
Nazwa w j. ang.	Security of computer networks

Koordynator	dr Mariusz Wojciechowski	Zespół dydaktyczny
		mgr Alfred Budziak mgr inż. Krystian Kurnik dr inż. Grzegorz Sokal dr Mariusz Wojciechowski
Punktacja ECTS*	3	

Opis kursu (cele kształcenia)

W ramach przedmiotu zdobędziesz teoretyczną wiedzę o polityce bezpieczeństwa, nauczysz się zarządzać ryzykiem i je analizować. Przedmiot obejmuje również zagadnienia związane z działaniem sieci VLAN, atakami na te sieci i ich zabezpieczaniem. Pozwoli Ci zrozumieć, do czego służą różne protokoły, z której strony haker może je zaatakować i jak się przed tym zabezpieczyć. A potem skonfigurujesz sieć w taki sposób, by atak na nią był maksymalnie utrudniony.

Kurs jest realizowany w języku polskim.

Warunki wstępne

Wiedza	Znajomość modelu ISO/OSI oraz protokołów warstwy aplikacji,
Umiejętności	Konfigurowanie urządzeń sieciowych w CLI oraz umiejętność linii komend,
Kursy	Wprowadzenie do sieci komputerowych,

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	Po zakończeniu kursu student:	
	W01: Ma wiedzę w zakresie zabezpieczania architektury systemów komputerowych i urządzeń sieciowych w lokalnych i rozległych sieciach komputerowych.	K_W04 K_W02 K_W07
	W02: Zna i rozumie zagadnienia dotyczące systemów informatycznych i sieci komputerowych oraz zasady ich organizacji i administracji.	
	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	Po zakończeniu kursu student:	
	U01: Potrafi opracować dokumentację, przedstawić prezentację i prowadzić dyskusję na temat zadania lub projektu, w szczególności związanych z bezpieczeństwem teleinformatycznym.	K_U01 K_U05 K_U06 K_U07 K_U08 K_U09 K_U10
	U02: Potrafi analizować i projektować protokoły, sieci i systemy teleinformatyczne, stosując właściwe metody, techniki i narzędzia oraz biorąc pod uwagę aspekty związane z bezpieczeństwem ich użytkowania.	
	U03: Potrafi konfigurować urządzenia i protokoły sieciowe oraz nimi zarządzać, mając na uwadze bezpieczeństwo danych.	

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	Po zakończeniu kursu student:	
	K01: Rozumie istotę pracy zespołowej, współdziałania z innymi osobami w ramach prac zespołowych i podejmowania różnych wiodących ról w interdyscyplinarnych zespołach oraz znaczenie konstruktywnej dyskusji w rozwiązywaniu problemów w obszarze cyberbezpieczeństwa.	K_K01 K_K02 K_K03 K_K05

Studia stacjonarne

Organizacja												
Forma zajęć	Wykład (W)	Ćwiczenia w grupach										
		A		K		L		S		P		E
Liczba godzin	20					30						

Studia niestacjonarne

Organizacja													
Forma zajęć	Wykład (W)	Ćwiczenia w grupach											
		A		K		L		S		P		E	
Liczba godzin	10					20							

Opis metod prowadzenia zajęć

Podczas pracy laboratoryjnej studenci będą rozwiązywać problemy zadane przez prowadzącego. Na ćwiczeniach na bieżąco weryfikowana będzie wiedza przekazywana podczas wykładów. Wykłady w formie prezentacji PowerPoint wspomagane platformą netacad.com firmy Cisco.

Formy sprawdzania efektów uczenia się

	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	X		X				X	
W02					X	X		X				X	
U01					X	X		X					
U02					X	X		X					
U03					X	X		X					
K01					X	X		X					

Kryteria oceny	Student otrzyma zaliczenie po uzyskaniu pozytywnego wyniku z wykonanych topologii sieciowych na zajęciach oraz napisania egzaminu zaliczeniowego.
----------------	---

Uwagi	
-------	--

Treści merytoryczne (wykaz tematów)

1. Podstawowa konfiguracja urządzeń
2. Koncepcja przełączania ramek
3. Wirtualne sieci LAN
4. Inter-VLAN routing
5. Protokoły drzewa opinającego
6. Agregacja portów
7. DHCP dla IPv4
8. Bezstanowa autokonfiguracja adresów i DHCP dla IPv6
9. Bezpieczeństwo sieci LAN
10. Sieci bezprzewodowa – koncepcja działania i podstawowa konfiguracja
11. Routing statyczny dla IPv4 i IPv6
12. Jednoobszarowy OSPFv2
13. Listy kontroli dostępu
14. Translacja adresów sieciowych
15. Wirtualne sieci prywatne i IPSec
16. Monitorowanie i zarządzanie siecią
17. Automatyzacja sieci
18. Ochrona sieci za pomocą rozwiązań IPS
19. Szyfrowanie z punktu widzenia użytkownika końcowego i administratora
20. Bezpieczeństwo stacji końcowych
21. Bezpieczeństwo poczty elektronicznej
22. Ochrona tożsamości
23. Typowy dzień analityka bezpieczeństwa
24. Łamanie haseł
25. Wykrywanie anomalii w sieci (i nie tylko!)
26. Zabezpieczenia w warstwie DNS

Wykaz literatury podstawowej

1. Sieci komputerowe. Biblia; Barrie Sosinsky; Helion 2011;
2. W drodze do CCNA. Zadania przygotowujące do egzaminu; Adam Józefiok; Helion 2012;
3. W drodze do CCNA. Część II; Adam Józefiok; Helion 2011;
4. CCNA 200-125. Zostań administratorem sieci komputerowych Cisco; Adam Józefiok; Helion 2017;
5. Praktyczne projekty sieciowe; Paweł Zaręba; Helion 2019;
6. 125 sposobów na bezpieczeństwo sieci. Wydanie II; Andrew Lockhart; Helion 2007;

Wykaz literatury uzupełniającej

1. Cisco CCNA 200-301. Kurs video. Podstawy sieci komputerowych i konfiguracji. Część 1; Adam Józefiok; Videopoint 2020;
2. Cisco CCNA 200-301. Kurs video. Administrowanie urządzeniami Cisco. Część 2; Adam Józefiok; Videopoint 2020;
3. Cisco CCNA 200-301. Kurs video. Administrowanie bezpieczeństwem sieci. Część 3; Adam Józefiok; Videopoint 2020;
4. Administrowanie sieciami Cisco. Kurs video. Przygotowanie do egzaminu CCNA/ICND2 200-105; Adam Józefiok; Videopoint 2016;
5. Bezpieczeństwo sieci Cisco. Przygotowanie do egzaminu CCNA Security 210-260; Adam Józefiok; Videopoint 2017;

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

Liczba godzin w kontakcie z prowadzącymi	Wykład	20
	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	10
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	0
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	5
	Przygotowanie do egzaminu/zaliczenia	5
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3

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

Liczba godzin w kontakcie z prowadzącymi	Wykład	10
	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	5
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	0
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	5
	Przygotowanie do egzaminu/zaliczenia	10
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3