BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH

Kod przedmiotu: BTS

Rodzaj przedmiotu: kierunkowy, obieralny

Specjalność: Technologie internetowe i sieci komputerowe

Wydział: Informatyki

Kierunek: Informatyka

Poziom studiów: pierwszego stopnia – VI poziom PRK

Profil studiów: praktyczny

Forma studiów: stacjonarna/niestacjonarna

Rok: 3

Semestr: 6

Formy zajęć i liczba godzin:

Forma stacjonarna

wykłady – 30

laboratorium – 20

Forma niestacjonarna

wykłady – 20

laboratorium – 15

Zajęcia prowadzone są w języku polskim.

Liczba punktów ECTS: 4

Osoby prowadzące:

wykład:
laboratorium:

---

1. Założenia i cele przedmiotu:

Celem przedmiotu jest przekazanie studentom wiedzy związanej z aspektami zapewnienia bezpieczeństwa dla komputerów znajdujących się wewnątrz lokalnej sieci komputerowej, przed zagrożeniami płynącymi z tejże sieci komputerowej.

2. Określenie przedmiotów wprowadzających wraz z wymaganiami wstępnymi:

Wymogi wstępne dotyczą wiedzy pobranej przez studentów na przedmiotach Systemy Operacyjne oraz Sieciowe Systemy Operacyjne.

3. Opis form zajęć

a) Wykłady

- **Treści programowe:**

1. Filtrowanie ruchu na przykładzie iptables w systemu GNU/Linux
2. Typy ataków sieciowych i metody obrony
3. Systemy wykrywania ataków IDS/IPS
4. Wykorzystanie usługi Proxy WWW do zabezpieczania lokalnej sieci komputerowej
5. Metody szyfrowania danych w sieciach komputerowych. Infrastruktura klucza publicznego
6. Przykłady wykorzystania infrastruktury klucza publicznego

- **Metody dydaktyczne**:

  Wykład prowadzony jest w formie prezentacji multimedialnej, uzupełnionej przykładami rozwiązywanymi w trakcie wykładu na tablicy oraz na rzutniku multimedialnym. W ramach wykładu, prowadzący wspólnie ze studentami omawiają praktyczne zastosowania prezentowanych treści.

- **Forma i warunki zaliczenia**:

  Warunkiem zaliczenia całości przedmiotu jest zdanie egzaminu w formie pisemnej.

- **Wykaz literatury podstawowej**:

1. Rash M.: Bezpieczeństwo sieci w Linuksie. Wykrywanie ataków i obrona przed nimi za pomocą iptables, psad i fwsnort. Wyd. Helion, Gliwice 2008
2. Kluczewski J.: Bezpieczeństwo sieci komputerowych. Praktyczne przykłady i ćwiczenia w symulatorze Cisco Packet Tracer. Piekary Śląskie: iTSt@rt Wydawnictwo informatyczne, 2019.
3. Kalsi T.: Bezpieczeństwo systemu Linux w praktyce. Receptury. Gliwice: HELION, cop. 2019.

- **Wykaz literatury uzupełniającej**:

1 Binnie Ch.: Linux Server. Bezpieczeństwo i ochrona sieci. Gliwice: HELION, cop. 2017.
2 Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka. T. 1. Gliwice: Helion, cop. 2019.
3 Scrimger R., LaSalle P., Leitzke C., Parihar M., Gupta M.: Biblia TCP/IP. Wyd. Helion, Gliwice 2002
4 Sijan Karanjit S.: TCP IP - Księga eksperta. Wyd. Helion, Gliwice 2002.
5 Comer D.: Sieci komputerowe i intersieci. Wyd. WNT, 2003.
6 Vademecum Teleinformatyka. IDG, 2004
7 Szmit M., Gusta M., Tomaszewski M.: 101 zabezpieczeń przed atakami w sieci komputerowej. Wyd. Helion, Gliwice 2005.
8 Ferguson N., Schneier B.: Kryptografia w praktyce. Wyd. Helion, Gliwice 2004
9 Adams C., Lloyd S.: PKI. Podstawy i zasady działania. Wyd. Helion, Gliwice 2007

b) Ćwiczenia laboratoryjne

- **Treści programowe:**

1. Podstawy konfiguracji zapory ogniowej opartej na aplikacji *Iptables* (dla pojedynczego hosta/serwera)
2. Konfiguracja zapory ogniowej opartej na aplikacji *Iptables* na ruterze dla ruchu przechodzącego z/do sieci lokalnej
3. Konfiguracja zapory ogniowej opartej na aplikacji *Iptables* na ruterze pod kątem realizacji dostępu do sieci Internet z wykorzystaniem usługi NAT
4. Stosowanie łańcuchów zagnieżdżonych w zaporze ogniowej opartej na aplikacji *Iptables*
5. "Oskryptowanie" zapory ogniowej opartej na aplikacji *Iptables*
6. Kompilacja jądra systemu GNU/Linux pod kątem implementacji zaawansowanych (dodatkowych) funkcjonalności dla aplikacji *Iptables*
7. Realizacja transparentnego proxy opartego na aplikacji Squid pod kątem zapewnienia bezpieczeństwa dla sieci lokalnej

8. Wykorzystanie aplikacji SNORT jako systemu IDS pod kątem zapewnienia bezpieczeństwa dla sieci lokalnej
9. Przykładowe wdrożenie i wykorzystanie infrastruktury klucza publicznego na bazie usługi Encrypted File System w otoczeniu sieciowym MS Windows

- **Metody dydaktyczne**:

W trakcie laboratorium prowadzący omawia zagadnienia związane z realizacją poszczególnych ćwiczeń, a następnie studenci samodzielnie realizują zadania określone przez prowadzącego.

- **Forma i warunki zaliczenia**:

Warunkiem zaliczenia przedmiotu jest uczestnictwo studenta na zajęciach laboratoryjnych oraz wykazanie się wiedzą z zakresu programu przedmiotu. Studenci uzyskują zaliczenie poprzez zdobycie określonej ilości punktów, przyznawanych za sprawozdania realizowane w trakcie zajęć, realizację projektu zabezpieczenia wskazanej lokalnej sieci komputerowej, oraz zaliczenia końcowego na ostatnich zajęciach. Zaliczenie otrzymuje student, który uzyskał określoną liczbę punktów, a o której informacja jest opublikowana na stronach WSTI. Ocenę z zaliczenia student uzyskuje w skali wskazanej w regulaminie studiów.

- **Wykaz literatury podstawowej**:

1. Rash M.: Bezpieczeństwo sieci w Linuksie. Wykrywanie ataków i obrona przed nimi za pomocą iptables, psad i fwsnort. Wyd. Helion, Gliwice 2008
2. Kluczewski J.: Bezpieczeństwo sieci komputerowych. Praktyczne przykłady i ćwiczenia w symulatorze Cisco Packet Tracer. Piekary Śląskie: iTSt@rt Wydawnictwo informatyczne, 2019.
3. Kalsi T.: Bezpieczeństwo systemu Linux w praktyce. Receptury. Gliwice: HELION, cop. 2019.

- **Wykaz literatury uzupełniającej**:

1 Binnie Ch.: Linux Server. Bezpieczeństwo i ochrona sieci. Gliwice: HELION, cop. 2017.
2 Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka. T. 1. Gliwice: Helion, cop. 2019.
3 Scrimger R., LaSalle P., Leitzke C., Parihar M., Gupta M.: Biblia TCP/IP. Wyd. Helion, Gliwice 2002
4 Sijan Karanjit S.: TCP IP - Księga eksperta. Wyd. Helion, Gliwice 2002.
5 Comer D.: Sieci komputerowe i intersieci. Wyd. WNT, 2003.
6 Vademecum Teleinformatyka. IDG, 2004
7 Szmit M., Gusta M., Tomaszewski M.: 101 zabezpieczeń przed atakami w sieci komputerowej. Wyd. Helion, Gliwice 2005.
8 Ferguson N., Schneier B.: Kryptografia w praktyce. Wyd. Helion, Gliwice 2004
9 Adams C., Lloyd S.: PKI. Podstawy i zasady działania. Wyd. Helion, Gliwice 2007

4. Opis sposobu wyznaczania punktów ECTS

a. forma stacjonarna

Forma zajęć	Formy aktywności studenta	Średnia ilość godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	30
	Czytanie wskazanej literatury	10
	Przygotowanie do zaliczenia	10
Ćwiczenia	Kontakt z nauczycielem	20
	Czytanie wskazanej literatury	5

	Realizacja projektu	25

Całkowita ilość godzin aktywności studenta	100
Liczba punktów ECTS dla modułu	4

b. forma niestacjonarna

Forma zajęć	Formy aktywności studenta	Średnia ilość godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	20
	Czytanie wskazanej literatury	15
	Przygotowanie do zaliczenia	15
Ćwiczenia	Kontakt z nauczycielem	15
	Czytanie wskazanej literatury	10
	Realizacja projektu	25

Całkowita ilość godzin aktywności studenta	100
Liczba punktów ECTS dla modułu	4

5. Wskaźniki sumaryczne

a. forma stacjonarna

a) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
   - Liczba godzin kontaktowych – 50
   - Liczba punktów ECTS – 2,0

b) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
   - Liczba godzin kontaktowych – 20
   - Liczba punktów ECTS – 2,0

b. forma niestacjonarna

a) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
   - Liczba godzin kontaktowych – 35
   - Liczba punktów ECTS – 1,4

b) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
   - Liczba godzin kontaktowych – 15
   - Liczba punktów ECTS – 2,0

6. Zakładane efekty uczenia się

Efekt przedmiotowy (Symbol)	Efekty kształcenia dla przedmiotu	Odniesienie do kierunkowych efektów uczenia się
BTS_01	… ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie zagrożeń płynących z sieci Internet do urządzeń w lokalnej sieci komputerowej i metod ich ograniczenia	K_W04, K_W06 K_U01, K_U18 K_K01

BTS_02	… ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie metod szyfrowania danych stosowanych w sieciach komputerowych, ze szczególnym uwzględnieniem Infrastruktury Klucza Publicznego	K_W04, K_W06 K_K01 K_U24
BTS_03	… potrafi stworzyć kod zapory ogniowej w oparciu o aplikację iptables dla wskazanego scenariusza sieci komputerowej	K_W04, K_W06 K_U02, K_U24
BTS_04	… potrafi zainstalować, skonfigurować i zarządzać systemem IDS w oparciu o aplikację SNORT	K_W06, K_U24
BTS_05	… potrafi wykorzystać funkcjonalność transparentnego Proxy WWW oraz Proxy POP/IMAP/SMTP do zwiększenia poziomu bezpieczeństwa w lokalnej sieci komputerowej	K_W06, K_U24
BTS_06	…… potrafi zrealizować projekt obejmujący zabezpieczenie lokalnej sieci komputerowej przed anomaliami płynącymi z sieci Internet, ze szczególnym uwzględnieniem aspektów pozatechnicznych, w tym środowiskowych, prawnych i ekonomicznych	K_W06, K_W12 K_W13, K_W14 K_W15, K_U02 K_U05, K_U11 K_U13, K_U15 K_U18, K_U19 K_K01, K_K03 K_U24

7. Odniesienie efektów uczenia się do form zajęć i sposób oceny osiągnięcia przez studenta efektów uczenia się

Efekt nr	Forma zajęć		Sposób sprawdzenia osiągnięcia efektu
	wykład	ćwiczenia	
BTS_01	*v*		Egzamin
BTS_02	*v*		Egzamin
BTS_03		*v*	Sprawdzian końcowy, sprawozdanie z laboratorium
BTS_04		*v*	Sprawdzian końcowy, sprawozdanie z laboratorium
BTS_05		*v*	Sprawdzian końcowy, sprawozdanie z laboratorium
BTS_06		*v*	Projekt, prezentacja osiągniętych wyników w projekcie

8. Kryteria uznania osiągnięcia przez studenta efektów uczenia się.

Efekt	Efekt jest uznawany za osiągnięty gdy:
BTS_01	student zaliczy pracę kontrolną w formie egzaminu pisemnego, zawierającego 3 pytania otwarte. Aby zaliczyć pracę kontrolną student musi uzyskać conajmniej 60% możliwych do zdobycia punktów, gdzie każde pytanie punktowane jest w skali od 1 do 10 punktów.
BTS_02	student zaliczy pracę kontrolną w formie egzaminu pisemnego, zawierającego 3 pytania otwarte. Aby zaliczyć pracę kontrolną student musi uzyskać conajmniej 60% możliwych do zdobycia punktów, gdzie każde pytanie punktowane jest w skali od 1 do 10 punktów.
BTS_03	a) student wykonał samodzielny projekt zwiększenia poziomu bezpieczeństwa wskazanego scenariusza korporacyjnej sieci komputerowej, oraz zaprezentował to rozwiązanie wykładowcy, potrafiąc również obronić zrealizowany dobór metod i narzędzi. b) student sporządził sprawozdania z ćwiczeń laboratoryjnych zawierające poprawnie wykonane założone ćwiczenia, c) student wykonał sprawdzian końcowy, realizowany w formie testu

BTS_04	a) student sporządził sprawozdania z ćwiczeń laboratoryjnych zawierające poprawnie wykonane założone ćwiczenia, b) student wykonał sprawdzian końcowy, realizowany w formie testu
BTS_05	a) student sporządził sprawozdania z ćwiczeń laboratoryjnych zawierające poprawnie wykonane założone ćwiczenia, b) student wykonał sprawdzian końcowy, realizowany w formie testu
BTS_06	student wykonał samodzielny projekt zwiększenia poziomu bezpieczeństwa wskazanego scenariusza korporacyjnej sieci komputerowej, oraz zaprezentował to rozwiązanie wykładowcy, potrafiąc również obronić zrealizowany dobór metod i narzędzi.