KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Cyberbezpieczeństwo [S1Teleinf1>CYBERB]

Przedmiot

Kierunek studiów
Teleinformatyka

Rok/Semestr
4/7

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
30

Laboratorium
15

Inne (np. online)
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

3,00

Koordynatorzy

dr hab. inż. Sławomir Hanczewski
slawomir.hanczewski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student przystępujący do tego kursu powinien posiadać podstawową wiedzę na temat protokołów stosu TCP/IP. Powinien rozumieć proces komunikacji między urządzeniami sieciowymi oraz znać podstawy systemów operacyjnych.

Cel przedmiotu

Celem kursu jest zapoznanie studentów z technikami w środowisku „piaskownicy” maszyn wirtualnych, które pozwalają na tworzenie, wdrażanie, monitorowanie i wykrywanie różnego rodzaju cyberataków. Kurs pozwala studentom zapoznać się z technikami wykorzystywanymi przez cyberprzestępców do obchodzenia zabezpieczeń danych, prywatności oraz bezpieczeństwa komputerów i sieci.

Przedmiotowe efekty uczenia się

Wiedza:
1. Student posiada usystematyzowaną wiedzę na temat kluczowych technologii bezpieczeństwa komputerowego i sieciowego.
2. Student ma podstawową, usystematyzowaną wiedzę z zakresu budowy, działania i standardów związanych z bezpieczeństwem komputerów i sieci.

3. Student zna środowisko maszyn wirtualnych umożliwiające tworzenie, implementację, monitorowanie i wykrywanie różnego rodzaju cyberataków.

Umiejętności:
1. Student potrafi dobierać odpowiednie technologie zabezpieczania komputerów i sieci.
2. Student posiada niezbędne umiejętności potrzebne do udaremnienia znanych i przyszłych cyberataków.
3. Student potrafi zastosować odpowiednie mechanizmy wykrywania nieuprawnionego dostępu do danych, systemów komputerowych i sieciowych.

Kompetencje społeczne:
1. Student zna granice własnej wiedzy i umiejętności, rozumie potrzebę dokształcania się w zakresie cyberbezpieczeństwa.
2. Student rozumie, że wiedza i umiejętności z zakresu cyberbezpieczeństwa bardzo szybko się dezaktualizują.
3. Student ma świadomość konieczności profesjonalnego podejścia do projektowania rozwiązań opartych na podejściu cyberbezpieczeństwa. Potrafi skutecznie uczestniczyć w projektach zespołowych.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu jest weryfikowana poprzez test ustny i/lub pisemny. Zagadnienia testowe, na podstawie których przygotowywane są pytania, przesyłane są studentom drogą mailową z wykorzystaniem uczelnianego systemu poczty elektronicznej. Test pisemny i/lub ustny składa się z 3 do 5 pytań, na które oczekiwana jest opisowa odpowiedź. Każda odpowiedź na pytanie jest oceniana w skali od 0 do 5 punktów. Każde pytanie jest równo punktowane. Próg zaliczenia: 50% punktów. W przypadku testu ustnego studenci losują pytania z zestawu 30 pytań. W przypadku testu pisemnego pytania wybiera prowadzący. Umiejętności nabyte w ramach laboratorium są na bieżąco weryfikowane. Na zakończenie każdego zajęcia laboratoryjnego poprawność konfiguracji urządzeń sieciowych oceniana jest w skali od 2 do 5. Ocena końcowa jest średnią ocen uzyskanych z poszczególnych zajęć laboratoryjnych.

Treści programowe

W trakcie wykładów prezentowane będą zagadnienia związane bezpieczeństwem: systemów operacyjnych, protokołów oraz urządzeń sieciowych. Ćwiczenia laboratoryjne: zagadnienia związane z bezpieczeństwem systemów operacyjnych (maszyny wirtualne), analiza ruchu sieciowego, bezpieczeństwo protokołów sieciowych.

Tematyka zajęć

1. W ramach wykładu omówione zostaną następujące tematy:
- Cyberbezpieczeństwo i SEO (Security Operation Center);
- Bezpieczeństwo sieci teleinformatycznych;
- Biały wywiad
- Bezpieczeństwo protokołów i usług sieciowych;
- Bezpieczeństwo infrastruktury sieciowej;
- Ataki sieciowe;
- Metody ochrony sieci;
- Kryptografia i infrastruktura klucza publicznego;
- Bezpieczeństwo i analiza punktów końcowych;
- Monitorowanie bezpieczeństwa.
2. W ramach zajęć laboratoryjnych realizowane będą następujące ćwiczenia laboratoryjne:
- Przygotowanie wirtualnego środowiska testowego;
- Używanie Wireshark do obserwowania ruchu sieciowego;
- skanowanie urządzeń sieciowych za pomocą programu Nmap;
- Wyszukiwanie podatności urządzeń i usług sieciowych;
- Testowanie bezpieczeństwa w sieciach lokalnych:
 * testy przełącznika ethernetowego,

* testy bezpieczeństwa urządzeń na ataki typu MitM,
* testy bezpieczeństwa serwerów DHCP.

Metody dydaktyczne

Wykład: prezentacja multimedialna ilustrowana przykładami na tablicy.
Ćwiczenia laboratoryjne: ćwiczenia praktyczne w grupach z wykorzystaniem komputerów osobistych i urządzeń sieciowych.

Literatura

Podstawowa:
William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Helion 2015
William Stallings, Network security essentials: applications and standards, Pearson Education, 2011.
William Stallingd, Systemy operacyjne. Architektura, funkcjonowanie i projektowanie, Helion, 2018

Uzupełniająca:
1. CCNA Cybersecurity Operations Companion Guide, Jun 15, 2018 by Cisco Press.
2. Raef Meeuwisse, Cybersecurity for Beginners, Lulu Publishing Services (May 14, 2015).
3. Lester Evans, Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners, Independently published (January 23, 2019).
4. Curriculum available on the cisco.netacad.net platform as part of the Cisco Network Academy run at the Institute of Communication and Computer Networks.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	86	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	45	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	41	1,00