KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Cyberbezpieczeństwo [S1EiT1E>CYBERB]

Przedmiot

Kierunek studiów
Elektronika i telekomunikacja/Electronics and Telecommunications

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
30

Laboratorium
15

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

3,00

Koordynatorzy

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@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 i znać podstawy systemów operacyjnych.

Cel przedmiotu

Celem modułu jest zapoznanie studentów z technikami stosowanymi w środowisku " sandbox" maszyny wirtualnej. która pozwala im tworzyć, wdrażać, monitorować i wykrywać różne rodzaje cyberataków. Moduł pozwala studentom zapoznać się z technikami wykorzystywanymi przez podmioty stanowiące zagrożenie do naruszania danych, prywatności oraz bezpieczeństwa komputerów i sieci.

Przedmiotowe efekty uczenia się

Wiedza:
1. Student ma usystematyzowaną wiedzę na temat kluczowych technologii bezpieczeństwa komputerowego i sieciowego.
2. Student ma podstawową, usystematyzowaną wiedzę z zakresu budowy, działania i norm z tym

związanych bezpieczeństwo komputera i sieci.
3. Student zna środowisko maszyny wirtualnej umożliwiające tworzenie, wdrażanie, monitorowanie i wykrywać różne rodzaje cyberataków.

Umiejętności:
1. Student potrafi dobrać odpowiednie technologie i zabezpieczania komputerów i sieci.
2. Student posiada umiejętności niezbędne do udaremnienia znanych i przyszłych cyberataków.
3. Student potrafi zastosować odpowiednie mechanizmy wykrywania nieautoryzowanego dostępu do danych, komputera i innych
systemy sieciowe.

Kompetencje społeczne:
1. Student zna granice własnej wiedzy i umiejętności, rozumie potrzebę dalszego szkolenia z zakresu cyberbezpieczeństwa.
2. Student rozumie, że wiedza i umiejętności z zakresu cyberbezpieczeństwa stają się przestarzałe bardzo szybko.
3. Student ma świadomość konieczności profesjonalnego podejścia do projektowania rozwiązań opartych na cyberbezpieczeństwie
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 na kolokwium ustnym i/lub pisemnym.
Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania, przesyłane są studentom drogą mailową z wykorzystaniem systemu uczelnianej poczty elektronicznej.
Kolokwium ustne i/lub pisemne obejmuje od 3 do 5 pytań, na które oczekuje się odpowiedzi opisowej. Każda odpowiedź na pytanie jest oceniana w skali od 0 do 5 punktów. Każde pytanie jest równo punktowane. Próg zaliczeniowy: 50% punktów.
W przypadku kolokwium ustnego studenci losują pytania ze zbioru 30 pytań. W przypadku kolokwium pisemnego pytania są zadawane przez prowadzącego.
Umiejętności nabyte w ramach zajęć laboratoryjnych weryfikowane są na bieżąco. Na każdych zajęciach laboratoryjnych oceniana jest poprawność wykonania ćwiczeń w skali od 2 do 5. Ocena końcowa jest średnią ocen uzyskanych z poszczególnych zajęć laboratoryjnych.Ocena końcowa jest średnią ocen uzyskanych z poszczególnych zajęć laboratoryjnych.

Treści programowe

- Cyberbezpieczeństwo i Security Operation Center;
- Zasady bezpieczeństwa sieci;
- Bezpieczeństwo systemu operacyjnego Windows;
- Bezpieczeństwo systemu operacyjnego Linux;
- 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.

Tematyka zajęć

1. W ramach wykładu omówione zostaną następujące tematy:
- Cyberbezpieczeństwo i Security Operation Center;
- Zasady bezpieczeństwa sieci;
- Bezpieczeństwo systemu operacyjnego Windows;
- Bezpieczeństwo systemu operacyjnego Linux;
- 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 przeprowadzone zostaną następujące ćwiczenia laboratoryjne:
- Instalacja maszyny wirtualnej CyberOps Workstation;
- Monitorowanie i zarządzanie zasobami systemowymi w systemie Windows;
- Poruszanie się po systemie plików Linux i ustawienia uprawnień;
- Korzystanie z Wireshark do obserwacji ruchu sieciowego;
- Anatomia złośliwego oprogramowania;
- Szyfrowanie i deszyfrowanie danych przy użyciu narzędzia hakerskiego;
- Interpretacja danych HTTP i DNS w celu wyizolowania podmiotu zagrożenia.

Metody dydaktyczne

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

Literatura

Podstawowa
1. William Stallings, Cryptography and network security : principles and practice ; Pearson Education. 2014.
2. William Stallings, Network security essentials: applications and standards, Pearson Education, 2011.
Dodatkowa
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	60	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	55	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	35	1,00