AGH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Nazwa modułu: Wprowadzenie do inżynierii bezpieczeństwa

Rok akademicki: 2014/2015 Kod: IIN-1-781-s Punkty ECTS: 3

Wydział: Informatyki, Elektroniki i Telekomunikacji

Kierunek: Informatyka Specjalność: —

Poziom studiów: Studia I stopnia Forma i tryb studiów: Stacjonarne

Język wykładowy: Polski Profil kształcenia: Ogólnoakademicki (A) Semestr: 7

Strona www: —

Osoba odpowiedzialna: dr inż. Faber Łukasz (faber@agh.edu.pl)

Osoby prowadzące: Kurdziel Marcin (kurdziel@agh.edu.pl)
dr inż. Faber Łukasz (faber@agh.edu.pl)

Krótka charakterystyka modułu

Moduł prezentuje przekrojową i aktualną wiedzę z dziedziny inżynierii bezpieczeństwa. Prezentowane są zarówno klasy zagrożeń, ich konkretne przykłady i analizy jak i sposoby radzenia sobie z nimi.

Opis efektów kształcenia dla modułu zajęć

Kod EKM	Student, który zaliczył moduł zajęć wie/umie/potrafi	Powiązania z EKK	Sposób weryfikacji efektów kształcenia (forma zaliczeń)
Wiedza			
M_W004	Zna i rozumie podstawowe aspekty bezpieczeństwa systemów operacyjnych	IN1A_W08, IN1A_W09	Wykonanie ćwiczeń laboratoryjnych
M_W005	Zna i rozumie podstawowe aspekty bezpieczeństwa infrastruktury sieciowej i aplikacji webowych	IN1A_W06, IN1A_W05	Wykonanie ćwiczeń laboratoryjnych
M_W006	Posiada wiedzę niezbędną do samodzielnego zaprojektowania, wdrożenia i audytu polityki bezpieczeństwa w przedsiębiorstwie	IN1A_W13	Wykonanie ćwiczeń laboratoryjnych, Aktywność na zajęciach
M_W007	Posiada wiedzę dotyczącą współczesnych problemów związanych z bezpieczeństwem systemów informatycznych	IN1A_W13, IN1A_W14, IN1A_W08	Aktywność na zajęciach
Umiejętności			
M_U003	Potrafi przeprowadzić test penetracyjny bezpieczeństwa systemu informatycznego	IN1A_U17, IN1A_U09	Wykonanie ćwiczeń laboratoryjnych

M_U004	Potrafi skonfigurować bezpieczne środowisko udostępniania usług sieciowych i webowych	IN1A_U11, IN1A_U14	Wykonanie ćwiczeń laboratoryjnych
Kompetencje społeczne			
M_K002	Rozumie znaczenie i społeczną wagę problemów zapewniania bezpieczeństwa systemom informatycznym.	IN1A_K02	Aktywność na zajęciach
M_K003	Rozumie konsekwencje i wpływ na rozwój społeczeństwa systemów związanych z anonimowością, ukrywaniem informacji, peer-to-peer i systemami DRM	IN1A_K02	Aktywność na zajęciach

Matryca efektów kształcenia w odniesieniu do form zajęć

Kod EKM	Student, który zaliczył moduł zajęć wie/umie/potrafi	Forma zajęć										
		Wykład	Ćwiczenia audytoryjne	Ćwiczenia laboratoryjne	Ćwiczenia projektowe	Konwersatorium	Zajęcia seminaryjne	Zajęcia praktyczne	Zajęcia terenowe	Zajęcia warsztatowe	Inne	E-learning
Wiedza												
M_W004	Zna i rozumie podstawowe aspekty bezpieczeństwa systemów operacyjnych	+	-	+	-	-	-	-	-	-	-	-
M_W005	Zna i rozumie podstawowe aspekty bezpieczeństwa infrastruktury sieciowej i aplikacji webowych	+	-	+	-	-	-	-	-	-	-	-
M_W006	Posiada wiedzę niezbędną do samodzielnego zaprojektowania, wdrożenia i audytu polityki bezpieczeństwa w przedsiębiorstwie	+	-	+	-	-	-	-	-	-	-	-
M_W007	Posiada wiedzę dotyczącą współczesnych problemów związanych z bezpieczeństwem systemów informatycznych	+	-	-	-	-	-	-	-	-	-	-
Umiejętności												
M_U003	Potrafi przeprowadzić test penetracyjny bezpieczeństwa systemu informatycznego	-	-	+	-	-	-	-	-	-	-	-
M_U004	Potrafi skonfigurować bezpieczne środowisko udostępniania usług sieciowych i webowych	-	-	+	-	-	-	-	-	-	-	-
Kompetencje społeczne												

M_K002	Rozumie znaczenie i społeczną wagę problemów zapewniania bezpieczeństwa systemom informatycznym.	+	-	-	-	-	-	-	-	-	-	-
M_K003	Rozumie konsekwencje i wpływ na rozwój społeczeństwa systemów związanych z anonimowością, ukrywaniem informacji, peer-to-peer i systemami DRM	+	-	-	-	-	-	-	-	-	-	-

Treść modułu zajęć (program wykładów i pozostałych zajęć)

Wykład

1. Czym jest bezpieczeństwo?
Podstawowe pojęcia i problemy. Modele bezpieczeństwa. Przykłady standardów. OWASP.
2. Bezpieczeństwo systemów operacyjnych.
Typowe naruszenia bezpieczeństwa. Problemy uwierzytelniania i kontroli dostępu. Ograniczone środowiska wykonania. Delegacja uprawnień.
3. Bezpieczeństwo infrastruktury sieciowej.
Podatności protokołów i urządzeń sieciowych. Firewalle. Tunele VPN i Ipsec. Protokoły wspomagające bezpieczeństwo (DNSSEC itp.).
4. Bezpieczeństwo aplikacji i usług.
Złośliwe oprogramowanie, wirusy, błędy implementacji. Podatności oprogramowania: przepełnienie stosu, przepełnienie bufora itp.
5. Anonimowość, systemy peer-to-peer, ukrywanie informacji, OTG.
6. Audyt i monitoring.
Systemy IDS/IPS. Narzędzia analizy zabezpieczeń. Systemy audytu.
7. Polityki i zarządzanie bezpieczeństwem.
Procedury reagowania. Ewaluacja systemów.
8. Prawa autorskie i systemy DRM.
9. Reverse engineering i analiza powłamaniowa.

Ćwiczenia laboratoryjne

1. Wprowadzenie do testów penetracyjnych – skanowanie sieci.
2. Wprowadzenie do testów penetracyjnych – systemy operacyjne, usługi sieciowe.
3. Wprowadzenie do testów penetracyjnych – aplikacje typu web.
4. Ograniczone środowiska wykonania aplikacji (sandboxing).
5. Systemy wykrywania incydentów (IDS).
6. Sprzętowe wsparcie kryptografii i bezpieczeństwa: TPM, HSM, UEFI.
7. Multilevel security i systemy MAC na przykładzie SELinux.

Sposób obliczania oceny końcowej

Ocena końcowa z przedmiotu jest równa ocenie z laboratorium.
Każdy temat laboratorium oceniane jest w systemie punktowym.
Ocena z laboratorium jest ilorazem sumy punktów za poszczególne zajęcia laboratoryjne przez maksymalną sumaryczną ilość punktów. Następnie następuje konwersja wartości procentowej do oceny wg regulaminu studiów.

Wymagane jest uzyskanie ponad 50% możliwych punktów za każde zajęcia laboratoryjne.

Wymagania wstępne i dodatkowe
Zalecane jest uczestnictwo w przedmiocie Kryptografia.

Zalecana literatura i pomoce naukowe
1. Ross Anderson: Security Engineering, 2nd edition; Wiley, 2008
2. Jason Luttgens, Matthew Pepe, Kevin Mandia: Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej; Helion, 2016
3. Joseph Muniz, Aamir Lakhani: Kali Linux. Testy penetracyjne; Helion, 2014
Dodatkowe informacje o literaturze, zwłaszcza o artykułach dotyczących aktualnych wydarzeń, podawane są przez prowadzącego na wykładzie i w treści instrukcji do laboratoriów.

Publikacje naukowe osób prowadzących zajęcia związane z tematyką modułu
Nie podano dodatkowych publikacji

Informacje dodatkowe
Brak

Nakład pracy studenta (bilans punktów ECTS)

Forma aktywności studenta	Obciążenie studenta
Udział w wykładach	14 godz
Udział w ćwiczeniach laboratoryjnych	14 godz
Samodzielne studiowanie tematyki zajęć	28 godz
Przygotowanie do zajęć	28 godz
Sumaryczne obciążenie pracą studenta	84 godz
Punkty ECTS za moduł	3 ECTS