**Nazwa przedmiotu:**

Techniki bezpieczeństwa IT

**Koordynator przedmiotu:**

mgr inż. Rafał Urbanelis

**Status przedmiotu:**

Fakultatywny ograniczonego wyboru

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Informatyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

**Semestr nominalny:**

3 / rok ak. 2011/2012

**Liczba punktów ECTS:**

4

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład: | 15h |
| Ćwiczenia: | 15h |
| Laboratorium: | 0h |
| Projekt: | 0h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

brak

**Limit liczby studentów:**

**Cel przedmiotu:**

Celem przedmiotu jest nabycie praktycznych umiejetnosci metod zapobiegania, ostrzegania i obrony przed atakami IT na roznych poziomach:
zarowno systemowym jak i sieciowym (na roznych warstwach modelu OSI). Podczas zajec studenci poznaja metody atakow na cale sieci i indywidualne maszyny a takze metody obrony przed nimi. Uzyskanie swiadomosci zagrozen i bezpieczenstwa IT powoduje lepsze podejscie do projektowania systemow, sieci i aplikacji.

**Treści kształcenia:**

1, 2 – konie trojańskie, keyloggery, rootkity
co to są trojany; kto ich używa; podział i opis generacji koni trojańskich; przykłady i prezentacja; metody zabezpieczenia; omówienie przypadków wykorzystania trojanów przez policję; najnowsze trendy; co to są keyloggery; podział keyloggerów (hardware i software); zastosowania; zaawansowane keyloggery; metody zabezpieczenia; rootkity
3 – ataki MITM (man in the middle)
co to jest sniffer; przykłady oprogramowania audytującego; pokaz działania sniffera; omówienie znanych w historii ataków MITM; metody zabezpieczeń
4,5 – anonimowość w sieci
proxy – omówienie zasad działania; podział proxy i anonimowe proxy; proxy chaining; tunele; forwarding portów; przykłady serwisów i pokaz użycia tunelowania oraz proxy.
6 – prywatność i ochrona danych
szyfrowanie dysków: rodzaje i sposoby, preboot vs. szyfrowane kontenery; odzyskiwanie danych: kasowanie plików; metody odzyskiwania danych; echo magnetyczne; omówienie przypadków z życia
7 – hasła
metody łamania: brute force, słowniki; co to jest ripper; przykłady oprogramowania audytującego; przykłady oprogramowania dedykowanego do odzyskiwania haseł w danych programach; zasady tworzenia haseł; sposoby zabezpieczeń
8 – wlan
omówienie idei; podstawowe zasady; słabości algorytmu RC4; pokaz oprogramowania skanującego / audytującego; metody zabezpieczeń
9,10 – zaawansowane techniki inwigilacji
techniki inwigilacji na podstawie szumu elektromagnetycznego: Tempest - wprowadzenie; przykłady przecieków z wojska na temat Tempest; Echelon: wprowadzenie i prawdopodobne zasady działania; dowody na istnienie; Carnivore: prawdopodobny opis systemu FBI używanego do inwigilacji elektronicznej
11 – porty
podstawowy opis i definicja; skanery portów – pokaz oprogramowania audytującego; przykłady z życia; metody zabezpieczania: zasada działania firewalla, inne metody
12 – steganografia
zarys idei; sposoby ukrywania informacji; przecieki na temat używania steganografii; przykłady programów
13 – remailery
idea remailerów i cel ich istnienia; rodzaje remailerów; sposób działania remailerów na przykładzie remailerów typu cypherpunk; przykłady oprogramowania
14 – podsumowanie zajęć
typy i osobowości atakujących; typowe cele ataków; popełniane błędy; schematy działań; procedury bezpieczeństwa; przykłady z życia;

**Metody oceny:**

Przewidziane jest jedno zaliczenie w formie testu jednoznacznego wyboru. Wynik testu będzie miał bezpośredni wpływ na końcową ocenę z przedmiotu. Drugorzędny wpływ na ocenę będzie miała aktywność na zajęciach. Ocenę będzie można poprawić po indywidualnych konsultacjach. Łączną ocenę punktową przelicza się na stopnie według poniższych zasad:
a) 3.0 jeżeli uzyskali od 51 do 60 pkt.
b) 3.5 jeżeli uzyskali od 61 do 70 pkt.
c) 4.0 jeżeli uzyskali od 71 do 80 pkt.
d) 4.5 jeżeli uzyskali od 81 do 90 pkt.
e) 5.0 jeżeli uzyskali powyżej 90 pkt.

**Egzamin:**

**Literatura:**

1. Joel McNamara - Secrets of Computer Espionage: Tactics and Countermeasures, 2003
2. Michal Zalewski, Zbigniew Banach - Cisza w sieci: praktyczny przewodnik po pasywnym rozpoznawaniu i atakach pośrednich, 2005
3. Greg Hoglund, James Butler - Rootkity – Sabotowanie jądra systemu Windows, 2006
4. Damian Put, Wojciech Kowalczyk, Adam Wróbel, Paweł Bylina - Szkoła Hakerów, 2006

**Witryna www przedmiotu:**

**Uwagi:**

## Efekty przedmiotowe