**KARTA KURSU**
realizowanego na specjalności

**CYBERBEZPIECZEŃSTWO**

| | |
|---|---|
| Nazwa | **Nowoczesne protokoły i mechanizmy zabezpieczeń sieciowych** |
| Nazwa w j. ang. | Modern network security protocols and mechanisms |

| | | |
|---|---|---|
| Koordynator | Dr hab. Serhii Semenov, prof. UKEN | Zespół dydaktyczny |
| | | Dr hab. Serhii Semenov, prof. UKEN |
| Punktacja ECTS* | st. stacjonarne: 3<br>st. niestacjonarne: 3 | |

Opis kursu (cele kształcenia)

| |
|---|
| Celem kursu jest zapoznanie studentów z nowoczesnymi protokołami i mechanizmami zabezpieczeń sieci komputerowych poprzez praktyczne ćwiczenia w środowisku laboratoryjnym. W trakcie kursu uczestnicy poznają aktualne techniki analizy ruchu sieciowego, identyfikacji i przeciwdziałania typowym zagrożeniom (m.in. spoofing, MITM, DoS), a także podstawy ataków i metod obrony w sieciach przewodowych i bezprzewodowych. |

Warunki wstępne

| | |
|---|---|
| Wiedza | Podstawy działania sieci komputerowych i modelu OSI; Znajomość podstawowych protokołów komunikacyjnych (np. IP, TCP/UDP, DNS, HTTP); Ogólna orientacja w zakresie zagrożeń cyberbezpieczeństwa. |
| Umiejętności | Obsługa systemów operacyjnych (Windows i/lub Linux) na poziomie użytkownika; Podstawowa umiejętność korzystania z terminala i pracy z plikami tekstowymi; Umiejętność instalowania i uruchamiania prostych aplikacji sieciowych. |
| Kursy | Teoria bezpieczeństwa, Wprowadzenie do sieci komputerowych, Bezpieczeństwo sieci komputerowych, Wprowadzenie do systemów operacyjnych, Bezpieczeństwo systemów operacyjnych |

Efekty uczenia się

| Wiedza | Efekt uczenia się dla kursu | Odniesienie do efektów kierunkowych |
|---|---|---|
| | Po zakończeniu kursu student:<br>W01: | SC_W03 |

| Umiejętności | Efekt uczenia się dla kursu | Odniesienie do efektów kierunkowych |
|---|---|---|
| | Po zakończeniu kursu student:<br>U01: | SC_U03, SC_U04, SC_U05 |

| Kompetencje społeczne | Efekt uczenia się dla kursu | Odniesienie do efektów kierunkowych |
|---|---|---|
| | Po zakończeniu kursu student:<br>K01: rozumie potrzebę etycznego i odpowiedzialnego wykorzystywania wiedzy z zakresu bezpieczeństwa | SC_K02, SC_K03 |

**Studia stacjonarne**

| Organizacja | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Forma zajęć | Wykład (W) | Ćwiczenia w grupach | | | | | | | | | |
| | | A | K | L | S | P | Z | | | | |
| Liczba godzin | 10 | | | 30 | | | | | | | |

**Studia niestacjonarne**

| Organizacja | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Forma zajęć | Wykład (W) | Ćwiczenia w grupach | | | | | | | | | |
| | | A | K | L | S | P | Z | | | | |
| Liczba godzin | 10 | | | 20 | | | | | | | |

Opis metod prowadzenia zajęć

Zajęcia prowadzone są w formie laboratoriów komputerowych, podczas których studenci samodzielnie wykonują ćwiczenia praktyczne z zakresu analizy ruchu sieciowego, identyfikacji zagrożeń oraz konfiguracji podstawowych mechanizmów bezpieczeństwa. Wykorzystywane są rzeczywiste scenariusze ataków i obrony w bezpiecznym środowisku testowym (np. maszyny wirtualne, narzędzia open source).

Metody nauczania obejmują:

- instruktaż wprowadzający do każdego tematu,
- samodzielne rozwiązywanie zadań problemowych,
- pracę indywidualną i zespołową przy stanowiskach komputerowych,
- analizę przypadków (case study) oraz symulacje incydentów bezpieczeństwa,
- pracę z dokumentacją techniczną i raportowaniem wyników.

Zajęcia mają charakter praktyczny, aktywizujący studentów do krytycznego myślenia i podejmowania decyzji w sytuacjach zbliżonych do realnych warunków pracy w branży IT.

Formy sprawdzania efektów uczenia się

| | E – learning | Gry dydaktyczne | Ćwiczenia w szkole | Zajęcia terenowe | Praca laboratoryjna | Projekt indywidualny | Projekt grupowy | Udział w dyskusji | Referat | Praca pisemna (esej) | Egzamin ustny | Egzamin pisemny | Zadania problemowe |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| W01 | | | | | X | | | X | | | | | |
| W02 | | | | | X | | | X | | | | | |
| W03 | | | | | X | | | X | | | | | |
| U01 | | | | | X | | | X | | | | | |
| U02 | | | | | X | | | X | | | | | |
| U03 | | | | | X | | | X | | | | | |
| K01 | | | | | X | | | X | | | | | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K02 | | | | | X | | | X | | | | | |
| K03 | | | | | X | | | X | | | | | |

| | |
|---|---|
| Kryteria oceny | Ocena końcowa z kursu opiera się na:<br><br>Aktywności i zaangażowaniu podczas zajęć laboratoryjnych (30%)<br>– regularne uczestnictwo, praca indywidualna i zespołowa, udział w analizach przypadków oraz dyskusjach.<br>Wykonaniu ćwiczeń i zadań laboratoryjnych (70%)<br>– poprawność techniczna rozwiązań, jakość interpretacji wyników, zgodność z założeniami ćwiczeń, terminowość oddania.<br><br>Warunkiem zaliczenia kursu jest:<br>wykonanie wszystkich obowiązkowych zadań laboratoryjnych,<br>uzyskanie co najmniej 50% możliwych punktów. |

| | |
|---|---|
| Uwagi | |

Treści merytoryczne (wykaz tematów)

1 Analiza ruchu sieciowego przy użyciu Wiresharka
Podstawy sniffingu, przegląd i filtrowanie pakietów
2 Identyfikacja wrażliwych danych w ruchu HTTP
Wyszukiwanie loginów i haseł w pakietach (HTTP, FTP)
3 ARP Spoofing i ataki typu Man-in-the-Middle (MITM)
Symulacja przechwycenia ruchu między hostami
4 Podstawy MAC spoofingu i przepełnienie tablicy CAM
Zmiana adresu MAC i obserwacja efektu w sieci
5 Ataki i ochrona VLAN – VLAN Hopping
Teoria + demonstracja pakietów trunkowanych (np. PackETH)
6 Wprowadzenie do protokołu STP i ataki BPDU
Analiza manipulacji STP i konsekwencje dla topologii
7 Składanie pakietów ręcznie – PackETH, Scapy (prosty scenariusz)
Tworzenie pakietów typu ARP, STP, DHCP
8 Bezpieczna konfiguracja SSH i ochrona przed brute-force
Test połączenia, analiza logów, konfiguracja fail2ban
9 Analiza DNS i podstawy ataków typu DNS Spoofing
Ruch DNS w Wiresharku, wprowadzenie do dnschef
10 Zbieranie informacji o usługach – Nmap, OS fingerprinting
Prosty skan portów, rozpoznanie systemu i usług
11 Podstawy ataków DoS – SYN flood i UDP flood (symulacja)
Wykorzystanie narzędzi testowych w bezpiecznym środowisku
12 Wprowadzenie do bezpieczeństwa Wi-Fi
Przechwytywanie ramek, analiza beaconów i handshake
13 Podstawy OSINT i inżynierii społecznej
Ćwiczenia z rozpoznawania phishingu i zbierania informacji
14 Bezpieczna konfiguracja zapory systemowej (Windows/Linux)
Blokowanie aplikacji i portów, sprawdzenie działania
15 Symulacja ataku i obrony – analiza incydentu w klasie
Ćwiczenie końcowe: MITM + analiza logów + identyfikacja ataku

Wykaz literatury podstawowej


1. Charlie Kaufman, Radia Perlman, Michael Speciner, Ray Perlner, Network Security: Private Communication in a Public World 3rd Edition Published September 16, 2022 https://www.nist.gov/publications/network-security-private-communication-public-world-3rd-edition
2. The Tangled Web: A Guide to Securing Modern Web Applications by Michal Zalewski No Starch Press 2019 https://archive.org/details/thetangledwebaguidetosecuringmodernwebapplications/page/n17/mode/2up

3. RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3
4. RFC 6749/6750: The OAuth 2.0 Authorization Framework
5. RFC 5246: TLS 1.2 (всё ещё актуален)
6. RFC 4301-4309: Security Architecture for IP (IPsec)
7. RFC 2865: RADIUS Authentication Protocol
8. RFC 8261: Secure Zero Touch Provisioning (SZTP)

Wykaz literatury uzupełniającej

1. William Stallings, Lawrie Brown Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. Tom 1 Wydawnictwo: Helion -2019, 632 s
2. William Stallings, Lawrie Brown Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. Tom 2 Wydawnictwo: Helion - 2019, 624 s

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – **studia stacjonarne**

| | | |
|---|---|---|
| Liczba godzin w kontakcie z prowadzącymi | Wykład | 10 |
| | Konwersatorium (ćwiczenia, laboratorium itd.) | 30 |
| | Pozostałe godziny kontaktu studenta z prowadzącym | 10 |
| Liczba godzin pracy studenta bez kontaktu z prowadzącymi | Lektura w ramach przygotowania do zajęć | 10 |
| | Realizacja zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu | 15 |
| | Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna lub w grupie) | 15 |
| | Przygotowanie do egzaminu/zaliczenia | 20 |
| Ogółem bilans czasu pracy | | 100 |
| Liczba punktów ECTS w zależności od przyjętego przelicznika | | 3 |

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – **studia niestacjonarne**

| | | |
|---|---|---|
| Liczba godzin w kontakcie z prowadzącymi | Wykład | 10 |
| | Konwersatorium (ćwiczenia, laboratorium itd.) | 20 |
| | Pozostałe godziny kontaktu studenta z prowadzącym | 15 |
| Liczba godzin pracy studenta bez kontaktu z prowadzącymi | Lektura w ramach przygotowania do zajęć | 15 |
| | Realizacja zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu | 20 |
| | Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna lub w grupie) | 15 |
| | Przygotowanie do egzaminu/zaliczenia | 15 |
| Ogółem bilans czasu pracy | | 100 |
| Liczba punktów ECTS w zależności od przyjętego przelicznika | | 3 |