

# Wstęp do cyberbezpieczeństwa (WCYB)

## Moduł 1: Kali Linux | Wprowadzenie do testów penetracyjnych - rekonesans

Semestr: 19Z

**Termin oddania rozwiązań: 5.11.2019, godz. 23:59**

### Zadania zaliczeniowe

1. Wykonaj przykład przedstawiony w punkcie 1.4.1 skryptu Lab1 dla domeny `juniper.net`.
2. Skorzystaj z Wireshark do przeglądu zrzutu ruchu zawierającego aktywność sieci podczas próby logowania na swoją uczelnianą skrzynkę pocztową. W którym momencie następuje uzgodnienie sesji TCP ? W którym momencie sesja jest zamykana (sekwencja flag TCP: FIN (klient), FIN+ACK (serwer), FIN (serwer), FIN+ACK(klient) w kolejnych segmentach)?
3. Wykorzystaj narzędzie `tcpdump` do wykonania zadań:
  - Przechwycenie aktywności sieci podczas próby logowania na swoją uczelnianą skrzynkę pocztową.
  - W którym momencie następuje uzgodnienie sesji TCP ? W którym momencie sesja jest zamykana (sekwencja flag TCP: FIN (klient), FIN+ACK (serwer), FIN (serwer), FIN+ACK(klient) w kolejnych segmentach)?
  - W strumieniu TCP odnajdź sekwencję logowania
  - Użyj filtra wyświetlania, aby zobaczyć tylko ruch na porcie 443
  - Uruchom ponownie przechwytywanie, tym razem za pomocą filtra przechwytywania, aby zebrać tylko port 443.

(Jest to powtórzenie zadań 1-4 z punktu 1.5.1 skryptu Lab1 oraz zadania nr 2 powyżej)
4. Wybierz organizację i użyj Google, aby zebrać jak najwięcej informacji na jej temat.
5. Skorzystaj z operatora `filetype` i poszukaj interesujących dokumentów pochodzenia wybranej organizacji w zadaniu 4.
6. Ponownie wykonaj ćwiczenie w domenie Politechniki Warszawskiej. Czy możesz znaleźć wyciek danych, o którym nie wiedziałeś?
7. Za pomocą narzędzia `whois` systemu operacyjnego Kali Linux zidentyfikuj nazwy serwerów Politechniki Warszawskiej.
8. Znajdź serwery DNS dla domeny `megacorpone.com`.
9. Napisz mały skrypt Bash, aby spróbować przenieść strefę z `megacorpone.com`.
10. Użyj `dnsrecon`, aby spróbować przenieść strefę z `megacorpone.com`.