

# Bezpieczeństwo komputerowe

## Lista nr 2 (A)

Pamiętaj: zgodnie z obowiązującym prawem, nie możesz wykorzystać danych zdobytych w wyniku wykonywania poniższych zadań do uzyskania nieuprawnionego dostępu.

**Zadanie 1 (5 pkt)** Zadanie można wykonywać w grupach max 2-osobowych. Skonfiguruj w odpowiedni sposób laptopa, udaj się z nim w publiczne miejsce i udostępniij publicznie otwartą sieć bezprzewodową (przeprowadź testy z różnymi nazwami SSID). Sporządźcie raport zawierający:

1. listę poszukiwanych SSID sieci, do których chciały się podłączyć urządzenia;
2. statystykę określającą nazwę udostępnianej (przez Ciebie) sieci i liczbę urządzeń, które się do niej podłączyły (na podstawie pakietów DNS),
3. listę stron www odwiedzonych przez użytkowników sieci,
4. listę protokołów i usług, z których korzystali użytkownicy sieci - jeżeli protokół nie wykorzystywał szyfrowania, to sporządź listę usług/serwisów/stron do których możnaby było zdobyć dostęp wykorzystując przesłane niezaszyfrowane loginy i hasła.
5. mapę lokalizacji, z którymi łączyły się komputery (wykorzystaj do tego celu programy np: traceroute, visualroute itp.).

Raport ma być wiarygodny: tj. zostaniesz zostać poproszona/poproszony o pokazanie odpowiadających danych źródłowych.

**Zadanie 2 (10 pkt)** Napisz aplikację (skrypt) przechwytyjącą nieszyfrowane sesje www (wykorzystaj np. Wireshark). Program ma (1) nasłuchiwać ruch sieciowy, (2) wynajdywać identyfikatory sesji (dla predefiniowanych stron), a następnie (po wybraniu) (3) zmieniać odpowiednie wpisy w ciasteczkach Twojej ulubionej przeglądarki tak, aby można było się podszyć pod podsłuchaną sesję.

Wykorzystaj np. programy tcpdump i aircrack (dla sieci zabezpieczonych WEP/WPA). Możesz skorzystać z danych zebranych w zadaniu nr 1.