Ćwiczenie 4 Testy penetracyjne - rekonesans

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie według załączonego wzoru, zawierające obrazy odpowiednich okien, oraz wnioski i komentarze dotyczące realizowanych zadań.
Sprawozdanie w postaci elektronicznej należy oddać prowadzącemu zajęcia przed opuszczeniem laboratorium.

Przeprowadzić rekonesans, będący fazą wstępną testu penetracyjnego, w stosunku do dowolnie wybranej domeny.

1. Korzystając z usługi WHOIS dokonać próby uzyskania następujących informacji:
   - bloki sieci (zakresy przydzielonych adresów IP),
   - wykaz ważniejszych serwerów (zwłaszcza DNS),
   - właściciel/rejestrator domeny,
   - przynajmniej jeden kontakt administracyjny,
   - ewentualnie ważniejsze numery telefonów.

   Należy wykorzystać dwa dowolne serwery WHOIS dostępne poprzez klienta (przeglądarkę) WWW.

2. Przy pomocy programu ***tracert*** dokonać próby badania osiągalności wszystkich serwerów DNS badanej domeny.

3. Dokonać próby badania dwóch dowolnie wybranych serwerów DNS domeny. W czasie badania należy próbować uzyskać:
   - zawartość całego pliku strefowego,
   - zdefiniowane w bazie rekordy MX (serwery pocztowe),
   - zdefiniowane w bazie rekordy CNAME (aliasy),
   - zdefiniowane w bazie rekordy HINFO (rekordy informacyjne),

   Należy wykorzystać:
   - pracujący w trybie tekstowym program systemowy ***nslookup***,
   - przynajmniej jedną witrynę narzędziową udostępniającą moduł (usługę) typu ***lookup***.

Przeprowadzanie dalszych faz testu penetracyjnego jest zabronione. Będzie ono realizowane w sieci lokalnej. Naruszenie tego zakazu może spowodować poważne sankcje (patrz Kodeks Karny, którego wybrane artykuły dotyczące tzw. przestępstw komputerowych były przedstawiane na wykładzie). Osoba naruszająca powyższy zakaz (bez względu na miejsce i czas jego przekroczenia) może zostać ukarana usunięciem z zajęć i niedopuszczeniem do egzaminu.