Ćwiczenie 4 Testy penetracyjne - rekonesans

Przeprowadzić rekonesans będący fazą wstępną testu penetracyjnego w stosunku do dowolnie wybranej domeny*. W czasie rekonesansu należy zidentyfikować następujące informacje:

- nazwę domeny,
- bloki sieci (zakresy przydzielonych adresów IP),
- ważniejsze serwery (DNS, pocztowe, www i ewentualnie inne),
- rejestratora domeny,
- jeden kontakt administracyjny,
- ewentualnie ważniejsze numery telefonów.

W czasie rekonesansu należy wykorzystać:

- ogólnie dostępne serwisy wyszukiwawcze (np. onet, wp, altavista, yahoo),
- stronę WWW wybranej organizacji,
- zasoby ***whois***,
- inne dostępne źródła.

Programy, których użycie jest wymagane i powinno zostać udokumentowane:

- przeglądarka wykorzystana do pobrania informacji z wybranych serwisów *whois*,
- program ***NetScan*** (zakładka *whois*),
- program ***WS Ping ProPack*** (zakładka *whois* i *lookup*),
- program ***nslookup*** do próby pobrania informacji o wybranych komputerach badanej domeny z jej serwera DNS,
- program ***tracert*** do próby stwierdzenia, czy odkryte ważniejsze komputery w badanej domenie, rzeczywiście funkcjonują,
- ewentualnie dodatkowo inne.

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie zawierające opis wszystkich wykonanych czynności i uzyskanych w ten sposób informacji. Przy opisie czynności należy podać wprowadzane polecenia (nazwy programów i ich parametry) lub ustawienia zadawane w oknach dialogowych. W sprawozdaniu należy zamieścić również obrazy okien wykorzystywanych programów. W sprawozdaniu powinny znaleźć się też informacje o niepowodzeniach tzn. próbach, które nie dały rezultatu. Należy wyjaśnić przyczyny niepowodzenia. Dokonać również porównania wykorzystanych narzędzi.

Sprawozdanie w postaci elektronicznej należy przekazać prowadzącemu zajęcia przed opuszczeniem laboratorium.

* 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.