

Ćwiczenie 7 Enumeracja kont i aplikacji w systemie Windows 2000

1. Dokonać enumeracji kont własnego komputera, wykorzystując programy:

- *DumpSec*,
- *winfo*,
- *nbtDump*,
- *enum*,
- *userinfo*,
- *userDump*,
- *getacct*,
- *walksam* (z pakietu *RPCtools*).

W czasie enumeracji należy określić listę wykrytych kont, szczegółowe informacje dotyczące tych kont oraz informacje polityki ochrony haseł. Wyniki zebrać w tabeli. Strukturę tabeli należy opracować samodzielnie.

2. Dokonać identyfikacji kont przy pomocy programów:

- *getsid* (z pakietu NTRK),
- *user2sid*,
- *sid2user*.

W czasie identyfikacji należy uzyskać SID systemu korzystając z programów *getsid* i *usersid*. Następnie należy rozpoznać listę wszystkich kont i grup w systemie, korzystając z programu *sid2user*.

3. Dokonać enumeracji aplikacji na wybranym komputerze w sieci laboratoryjnej przy pomocy programów:

- *telnet*,
- *NetCat*,
- *DumpSec*.

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 wykorzystywanych okien. 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 oddać prowadzącemu zajęcia przed opuszczeniem laboratorium.