

Ćwiczenie 6 Testy penetracyjne - enumeracja systemu Windows

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.

Na swojej partycji ćwiczebnej utworzyć foldery o nazwie PUBLIC i PRIVATE a następnie udostępnić je w sieci pod takimi samymi nazwami. Po zakończeniu ćwiczenia należy usunąć oba foldery.

Zadanie 1.

Przy pomocy programu systemowego **NET VIEW** dokonać rozpoznania:

- listy domen i grup roboczych funkcjonujących w sieci, w której realizowane jest ćwiczenie,
- listy komputerów funkcjonujących w jednej z domen lub grup roboczych dostępnych w sieci, w której realizowane jest ćwiczenie,
- zasobów swojego komputera.

W sprawozdaniu należy zamieścić obrazy okien zawierających w/w raporty wraz ze stosownym komentarzem.

Zadanie 2.

1. Przy pomocy programu systemowego **NBTSTAT**, dokonać rozpoznania zasobów swojego komputera. Uruchomić program dwukrotnie: raz z opcją **-c** a następnie z opcją **-n**. W sprawozdaniu należy zamieścić obrazy okien zawierających uzyskane raporty. Dokonać interpretacji uzyskanych wyników. Do czego można wykorzystać informacje ujawnione przy pomocy programu **NBTSTAT**?
2. Sprawdzić możliwość utworzenia pustej sesji na wybranym komputerze w sieci, w której realizowane jest ćwiczenie, wprowadzając polecenie:

NET USE \\adres_komputera\IPC\$ "" /U:""

W sprawozdaniu należy zamieścić obraz okna zawierającego w/w komendę i wynik jej uruchomienia.

Zadanie 3.

Dokonać rozpoznania zasobów swojego komputera, wykorzystując niżej wymienione, pracujące w trybie tekstowym, programy z pakietu *Resource Kit*:

- **srvinfo**,
- **getmac**,
- **getsid**.

W sprawozdaniu należy zamieścić obrazy okien zawierających raporty uzyskane w wyniku uruchomienia w/w programów. Zinterpretować uzyskane wyniki. Do czego można wykorzystać informacje ujawnione przy pomocy tych programów?

Zadanie 4.

Dokonać rozpoznania zasobów wybranego komputera w sieci, w której realizowane jest ćwiczenie, wykorzystując niżej wymienione programy:

- **DumpSec** (3 dowolnie wybrane raporty)
- **enum** (opcje -P, -S, -L)
- **userinfo**

W sprawozdaniu należy zamieścić obrazy okien zawierających raporty uzyskane w wyniku uruchomienia w/w programów. Zinterpretować uzyskane wyniki. Do czego można wykorzystać informacje ujawnione przy pomocy tych programów?