Ćwiczenie 5 Testy penetracyjne - techniki skanowania

Celem ćwiczenia jest zapoznanie studentów z wybranymi technikami skanowania. Pierwsza grupa zadań polega na realizowaniu skanowania przy pomocy programu *nmap* z wykorzystaniem jawnie zadanych metod. W czasie skanowania, należy obserwować jest ruch sieciowy, korzystając z pomocy *snifera*. Zadaniem studentów jest identyfikacja w ruchu sieciowym, sekwencji pakietów charakterystycznych dla zastosowanej metody. Druga część zadań polega na uruchamianiu różnych skanerów i identyfikacja, na podstawie obserwowanego ruchu sieciowego, metody stosowanej przez skaner do wykrycia funkcjonujących w sieci komputerów, lub otwartych portów.

W niniejszym ćwiczeniu pod pojęciem *wybrany partner* należy rozumieć dowolny, lub wskazany przez prowadzącego komputer w sieci lokalnej. Nie wolno skanować komputerów poza siecią lokalną. Zakres skanowanych portów (130-140) dotyczy skanowania systemów Windows. W przypadku skanowania innych systemów należy dobrać zakres portów w ten sposób, aby obejmował zarówno porty zamknięte jak i otwarte.

W ramach przygotowania do ćwiczenia należy zapoznać się z udostępnionymi materiałami wykładowymi (prezentacja BSI-02a) oraz literaturą zaleconą przez wykładowcę przedmiotu (J. Scambray, S. McClure, G. Kurtz, *Haking zdemaskowany – Rozdział 2).* Dodatkowo należy zapoznać się z obsługą wszystkich programów, które wykorzystywane będą w trakcie realizacji ćwiczenia. Można w tym celu wykorzystać plik *Instrukcje* udostępniany z materiałami do ćwiczeń.

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.*

Zadanie 1 – skanowanie metodą połączeniową (*TCP connect scan*)

Dokonać skanowania portów 130÷140 (TCP) komputera wybranego partnera, metodą połączeniową (*TCP connect scan*). W tym celu w oknie wiersza poleceń uruchomić program ***nmap*** z opcją ***–sT*** (**`nmap -p 130-140 -PN -sT adres_ofiary`**). W trakcie skanowania, przy pomocy sniffera należy zbierać pakiety wymieniane pomiędzy komputerem skanującym a skanowanym.

W sprawozdaniu zamieścić obraz okna zawierającego raport programu ***nmap*** z przeprowadzonego skanowania oraz obrazy okien *sniffera* z uwidocznionymi i w czytelny sposób zaznaczonymi (np. kolorową ramką) sekwencjami wykrywania pojedynczego portu otwartego i zamkniętego. Scharakteryzować zastosowaną metodę i ocenić poprawność uzyskanych wyników.

Zadanie 2 – skanowanie metodą półotwartą (*TCP SYN scan*)

Dokonać skanowania portów 130÷140 (TCP) komputera wybranego partnera, metodą półotwartą (*TCP SYN scan*). W tym celu w oknie wiersza poleceń uruchomić program ***nmap*** z opcją ***–sS*** (**`nmap -p 130-140 -PN -sS adres_ofiary`**). W trakcie skanowania, przy pomocy sniffera należy zbierać pakiety wymieniane pomiędzy komputerem skanującym a skanowanym.

W sprawozdaniu zamieścić obraz okna zawierającego raport programu ***nmap*** z przeprowadzonego skanowania oraz obrazy okien *sniffera* z uwidocznionymi i w czytelny sposób zaznaczonymi (np. kolorową ramką) sekwencjami wykrywania pojedynczego portu otwartego i zamkniętego. Scharakteryzować zastosowaną metodę i ocenić poprawność uzyskanych wyników.

Zadanie 3 – skanowanie metodą UDP (*UDP scan*)

Dokonać skanowania portów 130÷140 (UDP) komputera wybranego partnera, metodą UDP (*UDP scan*). W tym celu w oknie wiersza poleceń uruchomić program ***nmap*** z opcją ***–sU*** (**`nmap -p 130-140 -PN -sU adres_ofiary`**). W trakcie skanowania, przy pomocy sniffera należy zbierać pakiety wymieniane pomiędzy komputerem skanującym a skanowanym.

W sprawozdaniu zamieścić obraz okna zawierającego raport programu ***nmap*** z przeprowadzonego skanowania oraz obrazy okien *sniffera* z uwidocznionymi i w czytelny sposób zaznaczonymi (np. kolorową ramką) sekwencjami wykrywania pojedynczego portu otwartego i zamkniętego. Scharakteryzować zastosowaną metodę i ocenić poprawność uzyskanych wyników.

Zadanie 4 – skanowanie metodą FIN (*stealth FIN*)

Dokonać skanowania portów 130÷140 (TCP) komputera wybranego partnera, metodą FIN (*TCP FIN scan*). W tym celu w oknie wiersza poleceń uruchomić program ***nmap*** z opcją ***–sF*** (**`nmap -p 130-140 -PN -sF adres_ofiary`**). W trakcie skanowania, przy pomocy sniffera należy zbierać pakiety wymieniane pomiędzy komputerem skanującym a skanowanym.

W sprawozdaniu zamieścić obraz okna zawierającego raport programu ***nmap*** z przeprowadzonego skanowania oraz obrazy okien *sniffera* z uwidocznionymi i w czytelny sposób zaznaczonymi (np. kolorową ramką) sekwencjami wykrywania pojedynczego portu otwartego i zamkniętego. Scharakteryzować zastosowaną metodę i ocenić poprawność uzyskanych wyników.

Zadanie 5 – detekcja metody skanowanie hostów

Dokonać skanowania sieci laboratoryjnej w celu określenia liczby i listy funkcjonujących komputerów. Wykorzystać należy program ***Network Scanner***. W trakcie skanowania, przy pomocy *sniffera* należy zbierać pakiety wysyłane i odbierane przez skaner.

W sprawozdaniu zamieścić obraz okna zawierającego raport programu ***Network Scanner*** z przeprowadzonego skanowania oraz obraz okna *sniffera*. W tym ostatnim powinny zostać w sposób czytelny zaznaczone (np. ramką) pakiety reprezentatywne dla zastosowanej metody skanowania. Zidentyfikować zastosowaną metodę skanowania.

Zadanie 6 – detekcja metod skanowania portów

Przy pomocy programów:

- ***SuperScan***,
- ***ScanLine (sl)***

dokonać skanowania portów 130÷140 (TCP) komputera wybranego partnera. W trakcie każdego skanowania, przy pomocy *sniffera* należy zbierać pakiety wysyłane i odbierane przez skaner.

W sprawozdaniu zamieścić obrazy okien zawierające raporty wykorzystywanych skanerów, z przeprowadzonych skanowań oraz odpowiadające im obrazy okien *sniffera*. W tych ostatnich powinny zostać w sposób czytelny zaznaczone (np. ramką) pakiety reprezentatywne dla zastosowanej metody skanowania. Zidentyfikować zastosowane metody skanowania.