Ćwiczenie 02c.4 Testy penetracyjne - techniki skanowania

Celem ćwiczenia jest zapoznanie studentów z wybranymi technikami skanowania. Pierwsza grupa zadań polega na realizowaniu skanowania przy pomocy określonych skanerów 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.

Podczas realizacji ćwiczenia należy wykorzystać dwie maszyny wirtualne opisane w pierwszym ogłoszeniu związanym z realizowanym kursem internetowym. W opisie ćwiczenia maszyna skanująca oznaczona jest symbolem A. Maszyna skanowana oznaczona jest symbolem B. Zakres skanowanych portów (130-140) dotyczy skanowania systemów Windows. Został on dobrany tak, aby obejmował zarówno porty zamknięte jak i otwarte. Ćwiczenie należy wykonywać, będąc zalogowanym na koncie administratora. Mechanizmy ingerujące w ruch sieciowy (np. zapora) powinny być wyłączone.

W ramach przygotowania do ćwiczenia należy zapoznać się z udostępnionymi materiałami wykładowymi oraz literaturą zaleconą przez wykładowcę przedmiotu. Dodatkowo należy zapoznać się z obsługą wszystkich programów, które wykorzystywane będą w trakcie realizacji ćwiczenia.

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie według załączonego wzoru, zawierające obrazy odpowiednich okien, oraz wnioski i komentarze dotyczące realizowanych zadań.

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

Zalogować się na konto administratora. Z komputera A dokonać skanowania portów 130÷140 (TCP) komputera B, metodą połączeniową (*TCP connect scan*). W tym celu w oknie wiersza poleceń (Windnows PowerShell) uruchomić program ***nmap*** z opcją ***-sT*** (**`nmap -p 130-140 -PN -sT adres_ofiary`**). Skanowanie uruchomić dwukrotnie w odstępie około 1 minuty. W trakcie drugiego skanowania, przy pomocy sniffera *Wireshark* należy zbierać pakiety wymieniane pomiędzy komputerem skanującym a skanowanym. W programie *Wireshark* należy wyłączyć kolorowanie pakietów (menu ***View***).

W sprawozdaniu zamieścić obraz okna zawierającego raport utworzony przez program ***nmap*** 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*)

Zalogować się na konto administratora. Z komputera A dokonać skanowania portów 130÷140 (TCP) komputera B, metodą półotwartą (*TCP SYN scan*). W tym celu w oknie wiersza poleceń (Windnows PowerShell) uruchomić program ***nmap*** z opcją ***-sS*** (**`nmap -p 130-140 -PN -sS adres_ofiary`**). Skanowanie uruchomić dwukrotnie w odstępie około 1 minuty. W trakcie drugiego skanowania, przy pomocy sniffera *Wireshark* należy zbierać pakiety wymieniane pomiędzy komputerem skanującym a skanowanym. W programie *Wireshark* należy wyłączyć kolorowanie pakietów (menu ***View***).

W sprawozdaniu zamieścić obraz okna zawierającego raport utworzony przez program ***nmap*** 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*)

Zalogować się na konto administratora. Z komputera A dokonać skanowania portów 130÷140 (UDP) komputera B, metodą UDP (*UDP scan*). W tym celu w oknie wiersza poleceń (Windnows PowerShell) uruchomić program ***nmap*** z opcją ***–sU*** (**`nmap –p 130-140 -PN -sU adres_ofiary`**). Skanowanie uruchomić dwukrotnie w odstępie około 1 minuty. W trakcie drugiego skanowania, przy pomocy sniffera *Wireshark* należy zbierać pakiety wymieniane pomiędzy komputerem skanującym a skanowanym. W programie *Wireshark* należy wyłączyć kolorowanie pakietów (menu ***View***).

W sprawozdaniu zamieścić obraz okna zawierającego raport utworzony przez program ***nmap*** 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*)

Zalogować się na konto administratora. Z komputera A dokonać skanowania portów 130÷140 (TCP) komputera B, metodą FIN (*TCP FIN scan*). W tym celu w oknie wiersza poleceń (Windnows PowerShell) uruchomić program ***nmap*** z opcją ***–sF*** (**`nmap –p 130-140 -PN -sF adres_ofiary`**). Skanowanie uruchomić dwukrotnie w odstępie około 1 minuty. W trakcie drugiego skanowania, przy pomocy sniffera *Wireshark* należy zbierać pakiety wymieniane pomiędzy komputerem skanującym a skanowanym. W programie *Wireshark* należy wyłączyć kolorowanie pakietów (menu ***View***).

W sprawozdaniu zamieścić obraz okna zawierającego raport utworzony przez program ***nmap*** 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 metod skanowania hostów

Zalogować się na konto administratora. Z komputera A dokonać skanowania dowolnej wybranej sieci lokalnej[1] w celu określenia liczby i listy funkcjonujących komputerów. Wykorzystać należy program ***NetScan***. Przed uruchomieniem skanera należy wybrać funkcję ***Program Options*** w menu ***Options***, W oknach wszystkich dostępnych zakładek „wyczyścić” wszystkie opcje wyboru. Skanowanie uruchomić dwukrotnie w odstępach nie dłuższych niż 1 minuta. W trakcie drugiego skanowania, przy pomocy sniffera *Wireshark* należy zbierać pakiety wysyłane i odbierane przez skaner. W programie *Wireshark* należy wyłączyć kolorowanie pakietów (menu ***View***).

W sprawozdaniu zamieścić obraz okna zawierającego raport utworzony przez program ***NetScan*** 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.

[1] W przypadku szczególnym, jeżeli warunki techniczne nie pozwalają na inne rozwiązanie, skanowana sieć lokalna może zostać ograniczona do komputera B.

Zadanie 6 – detekcja metod skanowania

Zalogować się na konto administratora. Z komputera A, przy pomocy programów ***nsc1.exe, nsc2.exe, nsc3.exe, nsc5.exe, nsc6.exe, nsc7.exe, nsc8.exe*** dokonać skanowania komputera B. Każde skanowanie uruchomić dwukrotnie w odstępie około 1 minuty. W trakcie drugiego skanowania, przy pomocy sniffera *Wireshark* należy zbierać pakiety wysyłane i odbierane przez skaner. W programie *Wireshark* należy wyłączyć kolorowanie pakietów (menu ***View***).

W sprawozdaniu zamieścić obrazy okien zawierające raporty utworzone przez wykorzystywane skanery, 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.

Składnia linii uruchomienia wykorzystywanych skanerów:
nsc*x* *adr_ip* *adr_ip* 133 140
gdzie: *adr_ip* - jest adresem IP skanowanego komputera
x – jest numerem skanera {1, 2, 3, 5, 6, 7, 8}

Przykład: **nsc5 192.168.1.3 192.168.1.3 133 140**