

Ćwiczenie 5 Testy penetracyjne - techniki skanowania

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.

Uwagi wstępne

1. Zainstalować pakiet **WinPcap** i sniffer **Ethereal**.
2. Podczas realizacji niektórych zadań konieczne będzie uruchomienie sniffera i analizowanie transmitowanych pakietów. W tym celu, po uruchomieniu programu, należy:
 - W menu **Capture** wybrać funkcję **Start**.
 - W oknie **Ethereal: Capture Options** włączyć opcje:
 - * **Update list of packets in real time**
 - * **Automatic scrolling in live capture**
 - W tym samym oknie można zdefiniować filtr ograniczający ilość zbieranych pakietów wpisując w polu **Capture Filter** następującą formułę:
host adresIP_swojego_komputera and host adresIP_komputera_skanowanego
 - Podczas realizacji niektórych zadań, może być przydatne definiowanie filtra ograniczającego ilość wyświetlanych pakietów (**Display Filter**). Definiowanie takiego filtra ułatwia kreator dostępny po naciśnięciu przycisku **Expression** w głównym oknie programu.
3. Uruchomić program **nmap** (bez parametrów) i zapoznać się ze składnią wywołania tego programu.

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

Dokonać skanowania portów 130÷140 komputera wybranego partnera, metodą połączeniową (**TCP connect port scan**). W tym celu w oknie wiersza poleceń uruchomić program **nmap** z opcją **-sT**. W trakcie skanowania, przy pomocy sniffera należy zbierać pakiety wymieniane pomiędzy obydwojema komputerami.

W sprawozdaniu zamieścić obraz okna zawierającego raport programu **nmap** z przeprowadzonego skanowania, oraz obrazy okien sniffera z uwidocznionymi i zaznaczonymi sekwencjami wykrywania pojedynczego portu otwartego i zamkniętego. W tych ostatnich powinny zostać w sposób czytelny zaznaczone (np. ramką) sekwencje pakietów reprezentatywne dla zastosowanej metody skanowania. Scharakteryzować zastosowaną metodę i uzyskane wyniki.

Zadanie 2 – skanowanie metodą półotwartą (TCP SYN stealth port scan)

Dokonać skanowania portów 130÷140 komputera wybranego partnera, metodą półotwartą (**TCP SYN stealth port scan**). W tym celu w oknie wiersza poleceń uruchomić program **nmap** z opcją **-sS**. W trakcie skanowania, przy pomocy sniffera należy zbierać pakiety wymieniane pomiędzy obydwojema komputerami.

W sprawozdaniu zamieścić obraz okna zawierającego raport programu **nmap** z przeprowadzonego skanowania, oraz obrazy okien sniffera z uwidocznionymi i zaznaczonymi sekwencjami wykrywania pojedynczego portu otwartego i zamkniętego. W tych ostatnich powinny zostać w sposób czytelny zaznaczone (np. ramką) sekwencje pakietów reprezentatywne dla zastosowanej metody skanowania. Scharakteryzować zastosowaną metodę i uzyskane wyniki.

Zadanie 3 – skanowanie metodą UDP (UDP port scan)

Dokonać skanowania portów 130÷140 komputera wybranego partnera, metodą UDP (*UDP port scan*). W tym celu w oknie wiersza poleceń uruchomić program **nmap** z opcją **-sU**. W trakcie skanowania, przy pomocy sniffera należy zbierać pakiety wymieniane pomiędzy obydwojema komputerami.

W sprawozdaniu zamieścić obraz okna zawierającego raport programu **nmap** z przeprowadzonego skanowania, oraz obrazy okien sniffera z uwidocznionymi i zaznaczonymi sekwencjami wykrywania pojedynczego portu otwartego i zamkniętego. W tych ostatnich powinny zostać w sposób czytelny zaznaczone (np. ramką) sekwencje pakietów reprezentatywne dla zastosowanej metody skanowania. Scharakteryzować zastosowaną metodę i uzyskane wyniki.

Zadanie 4 – skanowanie metodą FIN (stealth FIN)

Dokonać skanowania portów 130÷140 komputera wybranego partnera, metodą FIN (*Stealth FIN*). W tym celu w oknie wiersza poleceń uruchomić program **nmap** z opcją **-sF**. W trakcie skanowania, przy pomocy sniffera należy zbierać pakiety wymieniane pomiędzy obydwojema komputerami.

W sprawozdaniu zamieścić obraz okna zawierającego raport programu **nmap** z przeprowadzonego skanowania, oraz obrazy okien sniffera z uwidocznionymi i zaznaczonymi sekwencjami wykrywania pojedynczego portu otwartego i zamkniętego. W tych ostatnich powinny zostać w sposób czytelny zaznaczone (np. ramką) sekwencje pakietów reprezentatywne dla zastosowanej metody skanowania. Scharakteryzować zastosowaną metodę i uzyskane wyniki.

Zadanie 5 – detekcja metody skanowanie hostów

Dokonać skanowania sieci laboratoryjnej w celu określenia liczby i listy funkcjonujących komputerów. Wykorzystać należy program **NetScan** (tylko zakładka *NetScanner*). W trakcie skanowanie, przy pomocy sniffera należy zbierać pakiety wysyłane i odbierane przez skaner.

W sprawozdaniu zamieścić obraz okna zawierającego raport programu **Netscan** 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:

- **NetScan** (tylko zakładka *PortProbe*),
- **SuperScan**,
- **Fscan**,

dokonać skanowania portów 130÷140 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.