Ćwiczenie 7 Testy penetracyjne - ataki *DoS*

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.

Zasadnicza część ćwiczenia realizowana będzie w zespołach dwuosobowych. Komputer jednego studenta będzie pełnił rolę atakowanego a komputer drugiego, rolę atakującego. Na komputerze atakującym będą uruchamiane programy realizujące określone ataki typu *DoS*. Na komputerze atakowanym należy uruchomić program monitorowania wydajności ***Wydajność*** (*Performance*) z grupy narzędzi administracyjnych. W panelu szczegółów okna tego programu, na bieżąco powinien być prezentowany stan liczników:

Obiekt: ***Procesor*** (*Processor)*; Licznik: ***Czas procesora [%]*** *(%Processor Time)*
Obiekt: ***Interfejs sieciowy*** (*Network Interface)*; Licznik: ***Całkowita liczba bajtów/s*** (*Bytes Total/sec)*

Wykresy powinny być skalowane w sposób umożliwiający oglądanie szczegółów ich przebiegu. Program powinien być aktywny przez cały czas ćwiczenia. Na komputerze atakowanym cały czas powinien być również aktywny program ***Menedżer zadań*** *(Windows Task Manager).* Korzystać należy z okna pod zakładką ***Wydajność*** (*Performance*). Okna obu wymienionych programów powinny być obserwowane.

Zadanie 1 Atak *SynFlood*

1. Na komputerze atakowanym uruchomić *sniffer* ***Ethereal***, w trybie analizy *na bieżąco*. Pożądane jest włączenie filtra, który ograniczy ilość zbieranych pakietów. Filtr powinien ograniczać źródłowy i docelowy adres IP do adresu komputera atakowanego oraz numer portu źródłowego i docelowego do numeru atakowanego portu (np. *host 192.168.214.18 and port 25*). Na komputerze atakowanym uruchomić również program ***Netstat*** w trybie wyświetlania wszystkich połączeń i nasłuchujących portów.

   Z komputera atakującego przeprowadzić atak przy pomocy programu ***SYN***, uruchamianego z konsoli tekstowej. Atak przeprowadzić poprzez wysłanie 10 pakietów na jeden dowolnie wybrany, otwarty port komputera atakowanego. W czasie ataku kilkakrotnie odświeżyć obraz generowany przez program ***Netstat***. Po zakończeniu ataku zatrzymać programy ***Ethereal*** i ***Netstat***.

   W sprawozdaniu zamieścić charakterystyczne dla przeprowadzonego ataku obrazy okien programów ***Ethereal*** i ***Netstat*** uzyskanych po stronie atakowanego (np. w raporcie programu ***Netstat*** powinny zostać uwidocznione komunikaty ODEBRANO_SYN a w raporcie snifera, pakiety wymianiane pomiędzy komputerami w czasie ataku). Zaznaczyć na tych obrazach elementy istotne dla zrozumienia charakterystyki przeprowadzonego ataku. Skomentować wyniki.

2. Z komputera atakującego przeprowadzić atak przy pomocy programu ***SYN***. Atak przeprowadzić na jeden dowolnie wybrany, otwarty port komputera atakowanego. Zapamiętać obrazy okien programów ***Menedżer zadań*** *(Windows Task Manager)* i ***Wydajność*** (*Performance*) uzyskane po stronie atakowanego. Po 20 sekundach wzmocnić atak wprowadzając dodatkowego atakującego (z dodatkowego komputera). Również zapamiętać obrazy okien programów ***Menedżer zadań*** *(Windows Task Manager)* i ***Wydajność*** (*Performance*) uzyskane po stronie atakowanego. Po kolejnych 20 sekundach wzmocnić atak wprowadzając trzeciego atakującego. Zapamiętać obrazy okien programów ***Menedżer zadań*** *(Windows Task Manager)* i ***Wydajność*** (*Performance*) uzyskane po stronie atakowanego. Po kolejnych 20 sekundach przerwać atak. W czasie realizacji zadań wymienionych w tym punkcie nie należy uruchamiać programów ***Ethereal*** i ***Netstat***.

   W sprawozdaniu zamieścić charakterystyczne dla przeprowadzonego ataku obrazy okien programów ***Menedżer zadań*** *(Windows Task Manager)* i ***Wydajność*** (*Performance*) uzyskanych po stronie atakowanego. Zaznaczyć na tych obrazach elementy istotne dla zrozumienia charakterystyki przeprowadzonego ataku. Skomentować wyniki. W sprawozdaniu należy zamieścić również charakterystykę przeprowadzonego ataku odwołując się w niej do zamieszczonych w sprawozdaniu okien uzyskanych podczas realizacji punktów 1 i 2. jako ilustracji. Przedstawić wnioski z przedstawionych obserwacji.

Zadanie 2 Atak *UDP Flood*

1. Na komputerze atakowanym uruchomić *sniffer* ***Ethereal***, w trybie analizy *na bieżąco*. Pożądane jest włączenie filtra , który ograniczy ilość zbieranych pakietów w sposób opisany w zadaniu 1. Na komputerze atakowanym uruchomić również program ***Netstat*** w trybie wyświetlania statystyk protokołu UDP (opcja s i p).

   Z komputera atakującego przeprowadzić atak przy pomocy programu ***SUF***, uruchamianego z konsoli tekstowej. Atak przeprowadzić na jeden dowolnie wybrany port UDP komputera atakowanego. Atak ograniczyć do wysłania 10 pakietów (opcja n). W czasie ataku kilkakrotnie odświeżyć obraz generowany przez program ***Netstat***. Po zakończeniu ataku zatrzymać programy ***Ethereal*** i ***Netstat***.

   W sprawozdaniu zamieścić charakterystyczne dla przeprowadzonego ataku obrazy okien programów ***Ethereal*** i ***Netstat*** uzyskanych po stronie atakowanego. Zaznaczyć na tych obrazach elementy istotne dla zrozumienia charakterystyki przeprowadzonego ataku. Skomentować wyniki.

2. Z komputera atakującego przeprowadzić atak przy pomocy programu ***SUF***. Atak przeprowadzić na jeden dowolnie wybrany, port UDP komputera atakowanego. Zlikwidować opóźnienie pomiędzy wysyłanymi pakietami (0). Zapamiętać obrazy uzyskanych po stronie atakowanego okien programów ***Menedżer zadań*** *(Windows Task Manager)* i ***Wydajność*** (*Performance*). Po 20 sekundach wzmocnić atak wprowadzając dodatkowego atakującego. Również zapamiętać obrazy uzyskanych po stronie atakowanego okien programów ***Menedżer zadań*** *(Windows Task Manager)* i ***Wydajność*** (*Performance*). Po kolejnych 20 sekundach wzmocnić atak wprowadzając trzeciego atakującego. Zapamiętać obrazy uzyskanych po stronie atakowanego okien programów ***Menedżer zadań*** *(Windows Task Manager)* i ***Wydajność*** (*Performance*). Po kolejnych 20 sekundach przerwać atak. W czasie realizacji zadań wymienionych w tym punkcie nie należy uruchamiać programów ***Ethereal*** i ***Netstat***.

W sprawozdaniu zamieścić charakterystyczne dla przeprowadzonego ataku obrazy okien programów ***Menedżer zadań*** *(Windows Task Manager)* i ***Wydajność*** (*Performance*) uzyskanych po stronie atakowanego. Zaznaczyć na tych obrazach elementy istotne dla zrozumienia charakterystyki przeprowadzonego ataku. Skomentować wyniki. W sprawozdaniu należy zamieścić również charakterystykę przeprowadzonego ataku odwołując się w niej do zamieszczonych w sprawozdaniu okien uzyskanych podczas realizacji punktów 1 i 2. jako ilustracji. Przedstawić wnioski z przedstawionych obserwacji.

Zadanie 3 Badanie obciążalności zasobów

Przeprowadzić atak przy pomocy programu ***Assault*** dla kilku znacząco różnych natężeń wysyłanych pakietów (parametr PPS) i tej samej wielkości pakietu. Spróbować określić doświadczalnie poziom natężenia wysyłanych pakietów, przy którym daje się zauważyć istotne zwiększenie zużycia zasobów systemu atakowanego. Dokonać również próby doświadczalnego określenia granicznego poziomu natężenia wysyłanych pakietów po przekroczeniu, którego nie obserwuje się już dalszego wzrostu obciążenia zasobów systemu atakowanego. Wyjaśnić to zjawisko.

W sprawozdaniu należy zamieścić obrazy okien programów ***Menedżer zadań*** *(Windows Task Manager)* i ***Wydajność*** (*Performance*) uzyskane po stronie atakowanego w pięciu istotnych, rozróżnialnych przypadkach. Przedstawić wnioski z przedstawionych obserwacji.

Zadanie 4 Atak ***Land***

Ćwiczenie przeprowadzić identycznie jak w przypadku ataku ***SynFlood***. Jedynie podczas uruchamiania programu SYN należy wykorzystać dodatkową opcję (-S) określającą adres komputera pod który podszywa się atakujący. W przypadku ataku ***Land*** adres ten powinien odpowiadać adresowi komputera atakowanego. Sprawozdanie zredagować identycznie jak dla zadania 1.