Pasywna identyfikacja systemów operacyjnych na podstawie własności pakietów sieciowych

Mikołaj Koszowski 274392
Hubert Nowakowski 274415

Zadanie na poziom 4

W celu zidentyfikowania systemu operacyjnego hostów w sieci lokalnej użyto programu ***Nmap*** w połączeniu z biblioteką pythonową ***libnmap*** pozwalającą na łatwe parsowanie wyników wyszukiwania.

Program Nmap wysyła serię pakietów TCP i UDP do zdalnego systemu i analizuje bity uzyskanych odpowiedzi pod kątem odcisków palców (fingerprint) systemów operacyjnych porównując z odciskami zapisanymi w bazie zawierającej ponad 1500 znanych odcisków systemów operacyjnych.

Skan w ćwiczeniu został wykonany z użyciem flagi **-O**, która realizuje podstawowe skanowanie. Możliwe jest też zastosowanie innych opcji, które przeprowadzają bardziej agresywne skany, lub próbują przewidywać system operacyjny bardziej swobodnie w przypadku zbliżonych wyników dla kilku systemów. Program może zwrócić kilka systemów operacyjnych z prawdopodobieństwem poprawności wyniku. W ćwiczeniu jako wynik wybrano najbardziej prawdopodobny system operacyjny.

W tabeli 1 pokazane są wyniki skanu w sieci domowej. Skan poprawnie zidentyfikował kilka systemów, przykładowo komputer o nazwie „hal.home”. W przypadku systemu urządzenia „desktop-57bsmfm.home” poprawnie została zidentyfikowany rodzaj systemu operacyjnego, ale konkretna wersja (windows XP) została źle przypisana. Komputer „laptop-9lmh9grv.home” został źle zidentyfikowany, co prawdopodobnie wynika z ostrzejszych ustawień antywirusa zainstalowanego na urządzeniu. Podczas skanowania antywirus urządzenia powiadomił o serii ataków blokując urządzenie skanujące.

Program Nmap pozwala na uzupełnianie bazy odcisków przez użytkowników. W przypadku błędnej identyfikacji systemu, jeżeli wystarczająca ilość pakietów została odebrana w wyniku skanu, a użytkownik wie jaki system operacyjny był skanowany, możliwe jest dodanie nowego odcisku do bazy danych.

Name	OS	Accuracy [%]
funbox.home	WAP: Linux, Linux(2.6.X)	100
desktop-57bsmfm.home	general purpose: Microsoft, Windows(XP)	85
pc-3.home	general purpose: Linux, Linux(2.6.X)	100
pc-888.home	firewall: Fortinet, embedded	87
laptop-9lmh9grv.home	specialized: AVtech, embedded	87
hal.home	general purpose: Linux, Linux(3.X)	100

Tabela 1 Wyniki skanowania sieci lokalnej.

Kod użytego programu znajduje się w pliku *nmap_osscan.py* oraz pod linkiem https://github.com/Fisher16/KiBD