

# Szczepanik.org

Raporty i dokumentacja

## ***„Windows XP + Service Pack 2, a RAW sockets”***

Autor: Piotr Szczepanik  
<piotr@szczepanik.org>  
Data: 11 grudzień 2004

## Co to są *RAW sockets* (*gniazda surowe*) ?

Od strony oprogramowania komunikacja w sieci odbywa się za pomocą *gniazd* (*sockets*).

W przypadku standardowych gniazd TCP/IP – strumieniowych i bezpołączeniowych – to system operacyjny zajmuje się tworzeniem i wypełnianiem pakietów (np. wypełnianiem nagłówek) przy użyciu odpowiedniego protokołu sieciowego. Zwalnia to programistę z troszczenia się o najniższe warstwy aplikacji komunikacyjnej jak i zapewnia pewnego rodzaju ochronę przed modyfikacją elementarnych składników komunikacji.

W przypadku *gniazd surowych* (*RAW sockets*) dozwolona jest ręczna modyfikacja nagłówek, dzięki czemu możliwe jest, np. tworzenie własnych protokołów sieciowych czy też modyfikacje adresów źródłowych wysyłanych pakietów na takie, które nie należą do „maszyny” je tworzącej.

## Zmiany w obsłudze *RAW sockets* w Windows XP SP2.

Service Pack 2 wprowadza dwie zmiany w obsłudze *surowych gniazd*:

1. Brak obsługi wysyłania danych TCP za pomocą *RAW sockets*.
2. Datagramy UDP nie mogą być wysyłane, kiedy adres źródłowy datagramu jest inny niż adres interfejsu sieciowego go wysyłającego.

Według Microsoft’u zmiany te podyktowane są względami bezpieczeństwa (utrudniają one, m.in. *IP spoofing*). Oficjalne stanowisko firmy informowało również o tym, iż *RAW sockets* wykorzystywane były tylko przez narzędzia do przeprowadzania ataków sieciowych.

W rezultacie programy wykorzystujące *RAW sockets* (np. nmap) mogą nie funkcjonować prawidłowo na systemach Windows XP z zainstalowanym Service Pack 2.

Z pewnością taka zmiana jest sposobem walki z użytkownikami wykorzystującymi Windows XP do generowania „niebezpiecznego” ruchu sieciowego, których wiedza ogranicza się do umiejętności uruchomienia odpowiedniego programu. Natomiast nie powstrzyma to użytkowników przed skorzystaniem z systemów operacyjnych dających większą swobodę w ich wykorzystaniu.

Istnieje również możliwość napisania specjalnego sterownika komunikującego się bezpośrednio ze sterownikiem urządzenia sieciowego, który to umożliwi uzyskanie funkcjonalności *RAW sockets*.