Programowanie sieciowe

Instrukcja do laboratorium - LAB 09

IOCTL

Zadanie 1. Program if_index.c służy do demonstracji działania funkcji ioctl().

Uwaga: eksperymenty z programem if_index.c przeprowadzać na interfejsie, który nie jest używany przez sesję ssh (zdalny dostęp)

1. Przeanalizować kod, skompilować program
2. Uruchomić program, znaleźć indeks i adres MAC interfejsu Ethernet (domyślnie eth0) – zweryfikować odczyt adresu MAC poleceniem ip
3. Zmienić adres MAC interfejsu eth0 – zweryfikować zmianę adresu MAC poleceniem ip
4. Przywrócić oryginalny adres MAC interfejsu (UWAGA: Nieprzywrócenie poprzedniego adresu może skutkować utratą połączenia sieciowego na danym interfejsie)
5. Dołożyć możliwość przestawienia interfejsu w tryb PROMISCUS (w zależności od parametru wejściowego programu ustawić lub wyzerować flagę IFF_PROMISC (<net/if.h>) na interfejsie).
   Uwaga !!!: ustawiając flagę IFF_PROMISC **nie zmieniać stanu pozostałych flag** – np. zmiana flagi IFF_RUNNING wyłączy interfejs i zablokuje sieć w komputerze.

PF_PACKET

Zadanie 2. W grupach dwuosobowych. Programy muszą być wykonywane pomiędzy dwoma maszynami fizycznymi lub wirtualnymi znajdującymi się w jednej sieci. Programy pf_packet_snd_v1.c i pf_packet_rcv_v2.c realizują przesyłanie pakietów w warstwie kanałowej dla protokołu sieciowego o id=0x0801

1. Przeanalizować kod, zmienić w kodzie nazwę interfejsu sieciowego, po którym będą przesyłane pakiety (aktywna funkcja bind())
2. Wysłać i odebrać pakiet na adresie unicast pomiędzy komputerami – Uwaga: należy uaktualnić w kodzie adres MAC komputera docelowego lub skorzystać z programu pf_packed_snd_v2.c
3. Wysłać i odebrać pakiet na adresie broadcast

4. Wysłać i odebrać pakiet na adresie multicast (skorzystać z dostępnej grupy multicastowej w warstwie kanałowej – ip maddr show)
5. Podglądnąć stan gniazd typu PACKET komendą: ss -n -a -0 -p
6. Przerobić program odbierający w ten sposób, aby używał gniazda typu SOCK_DGRAM zamiast SOCK_RAW? Jakie informacje wyświetlane przez program będą dla niego niedostępne po dokonaniu zmian? Dlaczego adresy MAC są niepoprawne? Przerobić program tak, aby wyświetlał poprawnie wszystkie informacje.
7. Przesłać strukturę danych pomiędzy komputerami: np. strukturę adresową z adresami IPv6 interfejsu (sockaddr_in6). Zwrócić uwagę na sieciową kolejność bajtów. Wyświetlić zawartość przesłanej struktury po stronie wysyłającej i odbierającej.

Zadanie 3. Program pf_packet_rcv_v3.c realizuje przechwytywanie pakietów w warstwie kanałowej (L2) dla wszystkich protokołów warstwy sieciowej (L3), ale wypisuje dodatkowe informacje tylko dla IPv4 i UDP:

- przeanalizować kod, skompilować i uruchomić

- zmienić kod w ten sposób, aby przechwytywał pakiety tylko dla protokołu sieciowego IPv4

- zmienić kod w ten sposób, aby przechwytywał tylko pakiety IPv6 i wyświetlał dodatkowo następujące pola z pakietów IPv6/TCP (<netinet/tcp.h>):

1) adresy MAC: źródłowy i docelowy
2) adresy IPV6: źródłowy i docelowy
3) porty źródłowy i docelowy
4) flagi TCP

- zaimplementować funkcję, która umożliwia dołączenie się do grupy multicastowej w warstwie L2 za pomocą opcji gniazda PF_PACKET

- zaimplementować funkcję, która umożliwia dołączenie włączenie trybu PROMISC w karcie sieciowej za pomocą opcji gniazda PF_PACKET

Zadanie 4. Napisać program klienta i serwer usługi DAYTME za pomocą gniazd PF_PACKED z obsługą adresacji typu unicast, broadcast i multicast.

Zadanie 5. Napisać program, który będzie wysyłał pakiety TCP SYNC do dowolnego adresu IPv4 lub IPv6 z losowego adresu IPv4 lub IPv6 do ataku DoS.

Do przygotowania na następne zajęcia (LAB10):

1. Wiadomości z LAB09.

2. Wiadomości z wykładów od 7 do 10.

3. Gniazda surowe (RAW) i protokół ICMP.

Pytania sprawdzające:

1. Do czego służy funkcja ioctl() ? Jakie parametry karty sieciowej można zmieniać za jej pomocą?

2. Jakie operacje można wykonywać na karcie sieciowej za pomocą funkcji ioctl()?

3. Jak działa tryb PROMISCUOUS na karcie sieciowej?

4. Co oznacza włączenie trybu MONITOR na karcie sieciowej?

5. Jakie funkcje z API gniazd można użyć do wykonywania operacji na gnieździe w domenie PF_PACKET?

6. Jakie funkcje można użyć do wysyłania pakietów dla gniazda sieciowego w domenie PF_PACKET?

7. Do czego służy opcja PACKET_ADD_MEMBERSHIP dla gniazd w domenie PF_PACKET?

8. Jakie pola struktury adresowej sockaddr_ll należy obowiązkowo wypełnić wywołując funkcję bind() dla gniazda w domenie PF_PACKET?

9. Jakie funkcje spełnia funkcja connect() dla gniazd w domenie PF_PACKET?

10. Jakie funkcje spełnia funkcja connect() dla gniazd w domenie PF_PACKET?

11. W jaki sposób przestawić interfejs sieciowy w tryb PROMISCUOUS za pomocą gniazd sieciowych? (dwa sposoby)

12. Jakie pola struktury adresowej sockaddr_ll należy wypełnić wysyłając ramkę Ethernet za pomocą gniazda PF_PACKET ?

13. Jakie kroki należy wykonać w programie, aby można było odebrać pakiet na gnieździe PF_PACKET?

14 Jakie kroki należy wykonać w programie, aby można było odesłać pakiet na gnieździe PF_PACKET?

15. Czym rożni się gniazdo w domenie PF_PACKET typu SOCK_RAW od SOCK_DGRAM?

16. Jakie kroki należy wykonać w programie, aby można było odebrać pakiet na gnieździe PF_PACKET adresowany na adres typu multicast?

17. Jakie kroki należy wykonać w programie, aby można było odebrać pakiet na gnieździe PF_PACKET adresowany na adres typu broadcast?