

# Podśluchiwanie w sieciach z przełącznikami - ćwiczenie

Krzysztof Kozłowski

8 lutego 2005 roku

## Spis treści

<b>1</b>	<b>Wstęp</b>	<b>1</b>
<b>2</b>	<b>Podśluch...</b>	<b>1</b>
2.1	ARP flood . . . . .	1
2.1.1	Zalewanie pakietami . . . . .	2
2.1.2	Podśluch . . . . .	3
2.2	Inne metody . . . . .	4
<b>3</b>	<b>Konkluzja i obrona</b>	<b>4</b>

## 1 Wstęp

O ile podśluchiwanie w sieci opartej na koncentratorze (*hub*) nie stanowi problemu, to teoretycznie przełączniki (*switch*) powinny całkowicie to uniemożliwić. Przełącznik przekazuje zwykle (nie rozgłoszeniowe ani nie grupowe) pakiety bezpośrednio do adresata. W praktyce istnieją metody pozwalające obejść tę właściwość.

## 2 Podśluch...

Zadaniem podsłuchującego jest przechwycenie pewnych informacji przekazywanych pomiędzy dwoma komputerami. Wiele ciągle używanych protokołów (POP, SMTP, FTP) nie stosuje szyfrowania i dane użytkowników (uwierzytelnienie) przesyłane jest czystym tekstem.

### 2.1 ARP flood

Przełącznik chcąc przekazać dalej otrzymany pakiet ethernetowski sprawdzi w swojej tablicy, na jakim porcie fizycznym znajduje się adres MAC adresata pakietu. W przypadku, gdy takowego adresu nie posiada w tablicy

(nie komunikował się z tym interfejsem), TRANSMITUJE GO NA WSZYSTKIE PORTY (jak koncentrator).

### 2.1.1 Zalewanie pakietami

**Zalewanie pakietami** Właściwość tę możemy wykorzystać do naszych celów. Gdyby udało się wypełnić mnóstwem adresów MAC tablicę przełącznika, to siłą rzeczy będzie musiał przejść on do przesyłania pakietów na wszystkich swoich portach.

**Zmienny MAC** Osiągniemy to wysyłając ogromną ilość pakietów z różnych (zmieniających się) adresów MAC. Wystarczy jeden pakiet ICMP do jednego z komputerów w sieci lokalnej, po czym następuje zmiana adresu MAC na inny. Skrypt przedstawiający takie działanie umieszczam poniżej :

```
#!/bin/sh
# Skrypt wysylajacy pingi z roznych adresow MAC. Do zalania przelecznika
# i przepelnienia jego tablicy adresow MAC. Dziala tragicznie wolno :), ale
# pokazuje idee :).
#
# Copyright (C) 2005 Krzysztof Kozlowski

INTERFACE="fxp1"
for i in 1 2 3 4 5 6 7 8 9 0 A B C D E F
do
  echo i=$i
  for j in 1 2 3 4 5 6 7 8 9 0 A B C D E F
  do
    echo j=$j
    for k in 1 2 3 4 5 6 7 8 9 0 A B C D E F
    do
      echo k=$k
      for l in 1 2 3 4 5 6 7 8 9 0 A B C D E F
      do
        for x in 1 2 3 4 5 6 7 8 9 0 A B C D E F
        do
          for y in 1 2 3 4 5 6 7 8 9 0 A B C D E F
          do
            ifconfig $INTERFACE ether 00:0e:5c:$i$j:$k$l:$x$y
            # echo ether 00:0e:0c:$i$j:$k$l:$x$y
            ping -I #INTERFACE -c 1 192.168.0.2 > /dev/null
          done
        done
      done
    done
  done
done
```

```
done
done
done
```

**Skrypt** Skrypt ten w 6-ciu pętłach zmienia adres MAC karty sieciowej na następny (zwiększa go o 1) i wysyła jeden ping do komputera 192.168.0.2 (jedna z maszyn uczestniczących w podsłuchiwanej transmisji). Napisanie tego w shellu nie daje dobrego wyniku pod względem wydajności. Wysłanie tablicy jednego prostego przełącznika udało nam się przeprowadzić dopiero przy użyciu dwóch komputerów, aczkolwiek w przypadku równoległego uruchomienia kilku takich skryptów możliwe, że tylko jeden komputer wykonałby zadanie.

**macof** W drugiej części testów (podczas przeprowadzania ataku na rozbudowany przełącznik HP ProCurve Switch 2524 (J4813A)<sup>1</sup>) został użyty specjalny program do przeprowadzania "floodu". Dokładniej chodzi o *macof* z pakietu *dsniff* (z portów dla FreeBSD).

```
# macof -i INTERFEJS -d 192.168.0.2 -d 22
```

Przełącznik *-d*, czyli docelowy port, użyty został, aby pakiety generowane przez *macof* nie trafiały do podsłuchującego *tcpdumpa*.

Program spełnił swoje zadanie znakomicie i działał zdecydowanie lepiej niż wcześniej zaprezentowany skrypt. Generował on ogromny ruch pakietów TCP w takim stopniu, że w 100-megabitowej sieci przełącznik HP został wysycony w przeciągu kilkunastu-kilkudziesięciu sekund. Jedyną przeszkodą było bardzo duże zużycie zasobów maszyny i *tcpdump* reagował z dużym opóźnieniem (nawet rzędu minuty), ale żadnego pakietu nie zgubił. Sama sieć również miała z tego powodu problemy z funkcjonowaniem.

### 2.1.2 Podsłuch

**tcpdump** Po uruchomieniu skryptu zalewającego przełącznik pingami można przejść do próby podsłuchu. Realizuje się to *tcpdump*'em :

```
tcpdump -i INTERFEJS -X -s 0 port 21 or port 23
```

**FTP, telnet, POP...** W przypadku protokołu FTP powinniśmy ujrzeć zarówno proces logowania (USER, PASS) jak i wszystkie komendy wykonywane przez użytkownika. A gdy ich nie ujrzymy ? Oznaczać to może, że nie udało się nam przepełnić tablicy adresów MAC lub np. przełącznik ma kilka

---

<sup>1</sup>Patrz: <http://www.hp.com/rnd/products/switches/switch2524-2512/overview.htm>

tablic - dla każdego portu. W pierwszym przypadku należy nasilić bombardowanie pakietami ICMP ping i troszkę odczekać. W drugim pozostaje tylko stosowanie innych metod.

## 2.2 Inne metody

**ARP spoofing** Wartą uwagi metodą podsłuchu w sieci przełączanej jest ”*ARP Spoofing*”, czyli podszywanie się pod adres MAC. Możemy udawać zarówno ”ofiare”, czyli komputer, którego transmisję chcemy przechwycić, jak i trasownik w sieci lokalnej, aby ruch sieciowy był kierowany w naszą stronę.

W pierwszym przypadku, również poprzez wysyłanie np. ping’ówi, należy przekonać przełącznik do przekazywania nam pakietów przeznaczonych dla ofiary. Wiąże się to jednak z przerwaniem transmisji u samego poszkodowanego. Również sam przełącznik zaobserwuje zmiany adresu MAC pomiędzy różnymi swoimi portami.

Podszywanie się pod trasownik w sieci lokalnej możemy uzyskać poprzez rozgłoszenia ARP. Ta metoda wymaga od nas przekazywanie otrzymywanych pakietów dalej.

## 3 Konkluzja i obrona

Omówiona tu pokrótce metoda zalewania pakietami o zmiennych adresach MAC pozwala przeprowadzić skuteczny podsłuch w sieci z przełącznikiem. Tym samym przełącznik nie może być traktowany jako panaceum na wszelkie problemy z bezpieczeństwem wewnątrz sieci lokalnej. Jak zostało pokazane i bardzo drogi oraz rozbudowany (pełna kontrola przez SNMP) przełącznik można bardzo łatwo ”przepełnić” doprowadzając do przejścia w tryb zwykłego ”koncentratora”. Z punktu widzenia administratora sieci stanowi on jednak istotne dodatkowe zabezpieczenie - prosty, typowy podsłuch nie uda się. A ten aktywny, czyli wymagający konkretnych akcji ze strony podsłuchującego, możliwy jest do wykrycia.

**Wykrywanie** Zalewanie przełącznika powoduje ruch rzędu kilkudziesięciu lub kilkuset (w zależności od sieci jak i komputera przeprowadzającego atak) pakietów na sekundę (w sieci laboratoryjnej w pewnym momencie tak duże obciążenie przełącznika całkowicie uniemożliwiło komunikację pozostałych maszyn). Jednocześnie błyskawicznie zmienia się adres MAC jednej maszyny, co można bez trudu wykryć (podczas ćwiczenia zostały zaobserwowane ogromne ilości komunikatów wysyłanych przez jądro FreeBSD jednej

ze zwykłych maszyn z informacją o zmianie adresu MAC innego komputera).  
Obroną jest teoretycznie łatwa możliwość wykrycia takiej formy podsłuchu.