ZABEZPIECZENIE PRZED ZMIANĄ ADRESU IP PRZEZ UŻYTKOWNIKA

Andrzej Angowski
UCI, UMK Toruń

Wprowadzenie

Zgodnie z ujednoliconą polityką bezpieczeństwa wśród organizacji partnerskich projektu eduroam, na dostawcy usługi dostępu do sieci Internet spoczywa obowiązek przechowywania dostatecznej ilości informacji, aby być w stanie jednoznacznie powiązać adres fizyczny (MAC) karty sieciowej użytkownika z otrzymanym przez niego w momencie zalogowania adresem logicznym (IP). Aby tego dokonać administrator przechowuje informacje o transakcjach DHCP (zapisywany jest czas uzyskania dzierżawy, adres fizyczny (MAC) i adres logiczny (IP)) dokonywanych przez klienta. Problem pojawia się, gdy użytkownik zmieni adres IP. Wówczas tracona jest informacja o powiązaniu pomiędzy adresem IP i MAC. Z tej sytuacji są dwa wyjścia: logować każdy pakiet przechodzący przez firewall zapisując nie tylko informacje o adresie IP, ale też MAC lub wprowadzić mechanizm zabezpieczający przed zmianą adresu IP przez użytkownika.

Na Uniwersytecie Mikołaja Kopernika w Toruniu wybrano drugie rozwiązanie. Aby uniemożliwić zmianę adresu IP przez klienta standardowo firewall eduroam nie przekazuje pakietów z Internetu do eduroam i odwrotnie. Dopiero po udanej transakcji DHCP możliwa jest komunikacja klienta ze światem zewnętrznym. Zamiast standardowego serwera DHCP zwykle dołączanego do dystrybucji Linux'a (Internet Systems Consortium's DHCPD) zastosowano do tego celu dnsmasq (więcej na: http://thekelleys.org.uk/dnsmasq/doc.html), który umożliwia wywołanie skryptu w momencie uzyskania dzierżawy adresu IP z DHCP. W ten sposób ilość przechowywanych informacji potrzebna, aby sprostać wymaganiom nałożonym na dostawcę usługi dostępu do Internetu znacznie się zmniejszyła.

Wymagania

Aby wprowadzić powyższy schemat w życie potrzebny będzie serwer oparty na systemie Linux. Serwer będzie obsługiwał zapytania DHCP klientów, będzie także firewall'em i routerem dla klientów podłączonych do sieci eduroam.

Na Uniwersytecie Mikołaja Kopernika zastosowano maszynę klasy PC z procesorem Intel Pentium IV 1.6GHz, 512MB RAM. Na maszynie zainstalowano Fedorę Core 5.

W dalszej części zakładam, że na maszynie zainstalowano standardowy zestaw pakietów z dystrybucji Fedora Core 5. Serwer jest skonfigurowany i działa poprawnie jako router dla użytkowników sieci eduroam.

Konfiguracja standardowej polityki firewalla

W ustawieniu firewalla należy zmienić standardową politykę przekazywania pakietów z ACCEPT na DROP (lub REJECT). Aby tego dokonać wydajemy polecenie (jako root):

```
#> iptables -P FORWARD DROP
```

lub zmieniamy odpowiedni wpis w pliku `/etc/sysconfig/iptables`

```
#> vim /etc/sysconfig/iptables
```

z
`:FORWARD ACCEPT [0:0]`
na
`:FORWARD DROP [0:0]`
i restartujemy iptables poleceniem:

```
#> service iptables restart
```

Ponadto należy zadbać, aby standardowo łańcuch FORWARD nie posiadał żadnych reguł. Dla pewności wpisujemy z pozycji uprzywilejowanego użytkownika root:

```
#> iptables -F FORWARD
```

Instalacja oprogramowania dnsmasq (http://thekelleys.org.uk/dnsmasq/doc.html)

Standardowo oprogramowanie dnsmasq dołączone jest do dystrybucji Fedora Core 5 jako pakiet "extras". Wystarczy więc wpisać (znów jako root):

```
#> yum install dnsmasq
```

W ogólnym przypadku należy pobrać z http://www.thekelleys.org.uk/dnsmasq/ najnowszą wersję źródeł, rozpakować i zbudować pakiet za pomocą narzędzia "make" zgodnie z instrukcjami zawartymi wewnątrz spakowanych źródeł.

Konfiguracja środowiska

Ze względów bezpieczeństwa skrypt obsługujący dodawanie i usuwanie reguł z łańcucha FORWARD nie powinien być wywoływany jako użytkownik root. Do tego celu tworzymy użytkownika i grupę dnsmasq:

```
#> groupadd dnsmasq -g <GID>
#> useradd dnsmasq -u <UID> -g <GID> -M
```

gdzie <GID> oznacza nieużywany do tej pory w systemie identyfikator grupy, <UID> oznacza nieużywany jeszcze w systemie identyfikator użytkownika. Następnie w pliku /etc/shadow w miejsce hasła użytkownika dnsmasq wstawiamy "!!" aby uniemożliwić mu logowanie do systemu. Wykonujemy więc polecenia (jako root):

```
#> cp /etc/shadow /etc/shadow-kopia
#> vim /etc/shadow
```

Aby użytkownik dnsmasq miał możliwość manipulacji łańcuchem FORWARD niezbędne jest dodanie wiersza do pliku `/etc/sudoers`:

```
dnsmasq ALL=(root) NOPASSWD: /sbin/iptables -L FORWARD, \
/sbin/iptables -A FORWARD *, /sbin/iptables -D FORWARD *
```

za pomocą poleceń:

```
#> cp /etc/sudoers /etc/sudoers-kopia
#> vim /etc/sudoers
```

Przygotowanie skryptu obsługującego reguły łańcucha FORWARD

Najprostszy skrypt dodający i usuwający reguły z łańcucha FORWARD ma postać:

```
#!/bin/sh
##############################################
# Uniwersytet Mikołaja Kopernika w Toruniu  #
# Pracowania Sieci Uczelnianej              #
#                                           #
# Przykładowy skrypt zarządzający regułami  #
# firewalla sieci eduroam                   #
##############################################
#
# skrypt posiada trzy parametry:
# 1) add (nowa dzierżawa DHCP) |
#    del (wygasająca dzierżawa) |
#    old (odnowiona dzierżawa –
#      np. w wypadku restartu dnsmasq w czasie trwania dzierżawy)
# 2) adres MAC klienta
# 3) adres IP klienta otrzymany z DHCP

IPTABLES='/sbin/iptables'
EXT_INTERFACE=<EXTERNAL INTERFACE>
INT_INTERFACE=<INTERNAL INTERFACE>

# jeśli dzierżawa jest nowa ($1 = add) lub odnowiona ($1 = old)
# i nie ma jeszcze takiej reguły w łańcuchu FORWARD
# to pozwalamy na przekazywanie pakietów w obie strony.

if [ \( $1 = 'add' -o $1 = 'old' \) -a \
`sudo $IPTABLES -L FORWARD | grep -i -c " $3 "` -eq 0 ]
  then
  sudo $IPTABLES -A FORWARD -i $INT_INTERFACE -o $EXT_INTERFACE \
-m mac --mac-source $2 -s $3 -j ACCEPT
  sudo $IPTABLES -A FORWARD -o $INT_INTERFACE -i $EXT_INTERFACE \
-d $3 -j ACCEPT
fi
```

```
# jeśli dzierżawa wygasa ($1 = del)
# i istnieją reguły w łańcuchu FORWARD
# pozwalające na przekazywanie pakietów w obie strony
# to je usuwamy.

if [ $1 = 'del' -a \
`sudo $IPTABLES -L FORWARD | grep -i -c " $3 "` -ne 0 ]
  then
  sudo $IPTABLES -D FORWARD -i $INT_INTERFACE -o $EXT_INTERFACE \
-m mac --mac-source $2 -s $3 -j ACCEPT
  sudo $IPTABLES -D FORWARD -o $INT_INTERFACE -i $EXT_INTERFACE \
-d $3 -j ACCEPT
fi
```

gdzie <EXTERNAL_INTERFACE> to interfejs zewnętrzny (wyjście na świat), np. eth0, <INTERNAL_INTERFACE> to interfejs wewnętrzny (klienci eduroam), np. eth1

UWAGA! Sprawdzenie czy reguły już istnieją czy nie potrzebne jest w przypadku, gdy:

- Maszyna została zrestartowana, łańcuch FORWARD jest pusty. Przy starcie dnsmasq przywraca trwające dzierżawy (old) i próbuje usunąć te, które zdążyły wygasnąć w trakcie wyłączenia maszyny (del). Przy próbie usunięcia nieistniejącej reguły otrzymujemy błąd: iptables: Bad rule (does a matching rule exist in that chain?)
- Dnsmasq został zrestartowany, np. aby wprowadzić zmiany w konfiguracji dnsmasq, Reguły w łańcuchu FORWARD cały czas istnieją. Jak w poprzednim punkcie, przy starcie dnsmasq dopisuje reguły dla trwających dzierżaw (old) i usuwa te, których dzierżawy zdążyły wygasnąć w trakcie restartu dnsmasq (del). Następuje zdublowanie reguł.

Powyższe sprawdzenie istnienia reguł zapobiega obu sytuacjom.

Skrypt umieszczamy np. w katalogu /opt/local/dnsmasq/dnsmasq_event. Plik oraz katalog, w którym go umieszczamy dodatkowo zabezpieczamy przed niepowołanym dostępem:

```
#> chown dnsmasq:dnsmasq /opt/local/dnsmasq/
#> chmod 700 /opt/local/dnsmasq/
#> chown dnsmasq:dnsmasq /opt/local/dnsmasq/dnsmasq_event
#> chmod 700 /opt/local/dnsmasq/dnsmasq_event
```

Konfiguracja dnsmasq

Standardowo konfiguracja oprogramowania dnsmasq znajduje się w /etc/dnsmasq.conf. Minimalna konfiguracja dla potrzeb eduroam może być następująca:

```
##########################################
# Uniwersytet Mikołaja Kopernika w Toruniu #
# Pracowania Sieci Uczelnianej             #
#                                          #
# Przykładowy plik konfiguracyjny serwera  #
# dnsmasq (DHCP) sieci eduroam             #
##########################################
# Configuration file for dnsmasq.
#
# Format is one option per line, legal options are the same
# as the long options legal on the command line. See
# "/usr/sbin/dnsmasq --help" or "man 8 dnsmasq" for details.

# dnsmasq uruchamiany jest jako użytkownik dnsmasq, grupa dnsmasq
user=dnsmasq
group=dnsmasq

# wypisujemy interfejsy, na których nasłuchuje dnsmasq
interface=<INTERNAL_INTERFACE>
# wypisujemy interfejsy, na których _NIE_ nasłuchuje dnsmasq
except-interface=<EXTERNAL_INTERFACE>

# podajemy dokładnie, na których adresach
# dnsmasq powinien nasłuchiwać
listen-address=127.0.0.1
listen-address=<IP_ADDRESS>

# wymuszamy bindowanie określonego adresu dla usług
# zadeklarowanych powyżej
bind-interfaces

# ustawiamy domenę
domain=<DOMAIN>

# ustawiamy skrypt, który ma być uruchamiany
# przy uzyskaniu/wygaśnięciu dzierżawy DHCP
dhcp-script=/opt/local/dnsmasq/dnsmasq_event

# ustawiamy (umowną) nazwę sieci na mynetwork1,
# zakres adresów IP i okres dzierżawy DHCP
dhcp-range=mynetwork1,<LOWEST_IP>,<HIGHEST_IP>,2h

# serwer DHCP ma być "autorytatywny"
dhcp-authoritative
```

gdzie <EXTERNAL_INTERFACE> to interfejs zewnętrzny (wyjście na świat), np. eth0, <INTERNAL_INTERFACE> to interfejs wewnętrzny (klienci eduroam), np. Eth1, <IP_ADDRESS> to adres IP nadany interfejsowi <INTERNAL_INTERFACE>, <DOMAIN> to nazwa domeny pod którą pracować będą klienci eduroam, <LOWEST_IP> i <HIGHEST_IP> to najniższy i najwyższy dostępny adres IP w puli adresów przeznaczonej do przydzielenia dla klientów DHCP.

Następnie ustawiamy automatyczny start demona dnsmasq przy starcie systemu (jako root):

```
#> setup
```

-> “usługi systemowe” -> zaznaczamy opcje “dnsmasq”
lub

```
#> chkconfig --add dnsmasq
```

Uwagi dodatkowe

Oprogramowanie dnsmasq powstało głównie z myślą o małych i średnich sieciach za maskaradą. Integruje ono w sobie demona DHCP, ale także DNS. Dobrze więc jest wykorzystać go w swojej sieci jako serwer cache'ujacy zapytania DNS. Dla danych interfejsów standardowo obie usługi (DHCP i DNS) są wystawione. Istnieje możliwość wyłączenia funkcjonalności DHCP przy zachowaniu DNS za pomocą opcji w pliku dnsmasq.conf:

```
no-dhcp-interface=<INTERNAL_INTERFACE>
```

niestety nie ma możliwości zachowania funkcjonalności DHCP i wyłączenia DNS.