Zarządzanie bezpieczeństwem informacji - laboratorium
Dynamiczne reguły dostępu do usług

Celem ćwiczenia jest zdobycie umiejętności konfiguracji dynamicznych reguł dostępu do usług na bazie filtracji pakietów w systemie operacyjnym Linux. Ćwiczenie realizowane będzie w SO Linux w wersji Knoppix Live.

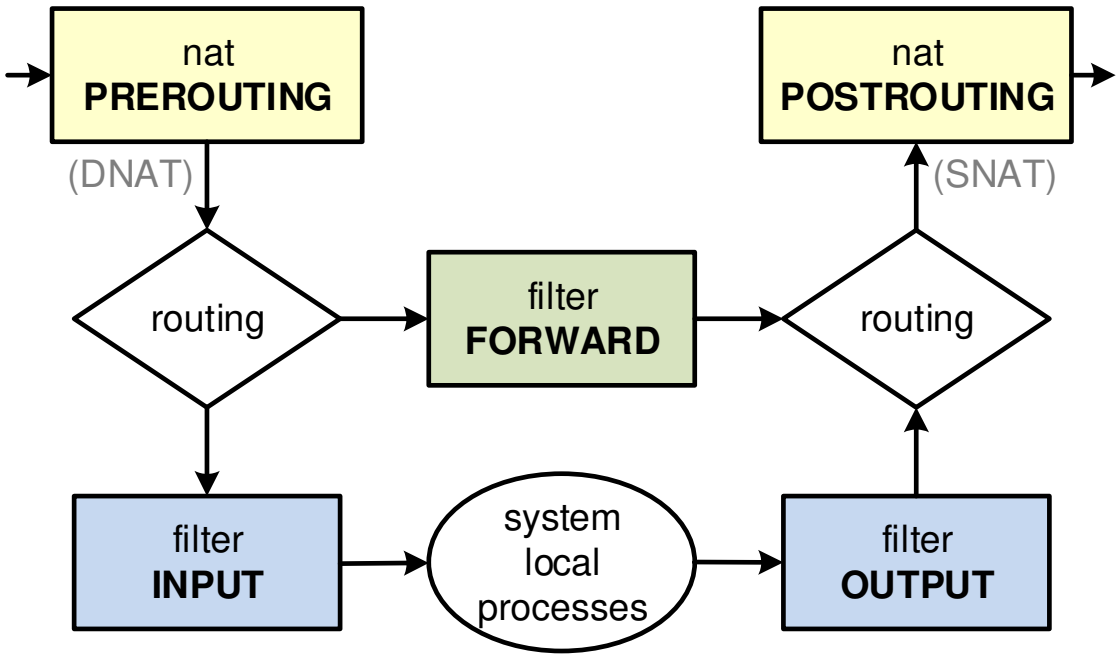
1. Czynności przygotowawcze

*Uwaga! W wersji Live systemu Knoppix usługa *syslog* jest domyślnie uruchomiona, a komunikaty pojawiają się na dwunastej konsoli (Ctrl-Alt-F12). Powrót do konsoli graficznej (Ctrl-Alt-F5).

1.1. Minimalny zestaw reguł zapory sieciowej

```
#wyczyszczenie wszystkich poprzednich reguł
iptables -F
iptables -X
#ustalenie domyślnych polityk
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
#zezwolenie na odpowiedzi własnych żądań
iptables -A INPUT -j ACCEPT -m state --state ESTABLISHED,RELATED
```

1.2. Trasy datagramów i standardowe filtry systemowe



1.3. Uruchomienie przykładowych usług

Dla potrzeb ćwiczenia należy uruchomić usługę dostępu zdalnego przez SSH i serwera webowego Apache

```
service sshd start
service apache2 start
```

2. Dostęp dynamiczny do usług z wykorzystaniem algorytmu knok-knok

2.1. Opis

Algorytm *knok-knok* (puk-puk) pozwala domyślnie utrzymywać zamknięte porty usług dostępnych w systemie, co uniemożliwia dostęp do tych usług z zewnątrz. Przez zastosowanie odpowiedniej sekwencji prób nawiązania połączeń sieciowych z innymi, selektywnie wybranymi portami, można dla wybranego adresu źródłowego, na określony, krótki czas umożliwić nawiązanie nowego połączenia z usługą. Sekwencja kolejności i wartości numerów portów pełni rolę tajnego hasła otwierającego dostępu do usługi. Aby uniemożliwić przypadkowe otwarcie dostępu do usługi zaleca się używanie numerów portów większych od portu usługi i w sekwencji nierosnącej.

2.2. Implementacja

Dynamiczne reguły korzystają z modułu *recent* systemowego filtra datagramów. Moduł *recent* pozwala zapamiętywać, zapominać i testować czas wpisu adresów źródłowych datagramów IP przechodzących przez filtry.

Typowym działaniem jest zapamiętanie adresu wykonującego pierwszą w sekwencji próbę połączenia na liście numer 1, zapamiętanie adresu wykonującego drugą próbę połączenia na liście numer 2 tylko jeśli adres jest na liście numer 1 nie dłużej niż np. 30 sek. i wpuszczenie do usługi wyłącznie klientów z adresów na liście numer 2 jeśli znajdują się na niej nie dłużej niż określony czas. Wpisując adres na listę warto go usunąć z pozostałych list.

Przydatne polecenia:

```
#utworzenie nowego filtru iptables
iptables -N KNOK1
#przekierowanie określonego ruchu do filtru
iptables -A INPUT -p tcp --dport 12345 -j KNOK1
#zapamiętanie adresu źródłowego datagramu w filtrze na listę
iptables -A KNOK1 -m recent --set --name AUTH1
#odrzucenie wszystkich datagramów w filtrze
iptables -A KNOK1 -j DROP
#usunięcie adresu z listy bez modyfikacji datagramu
iptables -A INPUT -m recent --name AUTH1 --remove
#przepuszczenie datagramu z zapamiętanego adresu źródłowego
ipatables -A INPUT -j ACCEPT -m recent --rcheck --name AUTH1 --seconds 30
```

Zapamiętane adresy IP można sprawdzić w pliku /proc/net/xpt_recent/AUTH1

2.3. Zadania

Zaimplementować zestaw reguł iptables umożliwiających dostęp do usług SSH i WWW po wykonaniu sekwencji dwóch prób nawiązania połączenia kolejno z portami 23456 i 12345.

Sprawdzić poprawność działania.

Sprawdzić brak możliwości skorzystania z usług bez procedury knok-knok i po skanowaniu otwartych portów programem nmap.

3. Dynamiczne blokowanie dostępu do systemu dla hostów

3.1. Opis

Fail2ban jest narzędziem pomagającym zabezpieczyć usługi pracujące w systemach Linux. Zabezpieczenie polega na dynamicznym wprowadzaniu do reguł zapory blokad uniemożliwiających korzystanie z usług i systemu dla klientów powodujących błędy np. uwierzytelniania. Realizowane jest to przez ciągłe skanowanie logów systemowych albo logów usługi (aplikacji) w poszukiwaniu określonych błędów. Przekroczenie zadanej liczby błędów w określonym czasie powoduje aktualizacje ustawień zapory tak, aby uniemożliwić połączenia z adresu IP. Fail2ban dostarczany jest z predefiniowanymi konfiguracjami dla popularnych usług i aplikacji. Możliwe jest również samodzielne wskazanie pliku dziennika, wyrażenie regularnego oraz parametrów takich jak liczba błędów, czas blokady, metoda powiadomienia itp.

3.2. Czynności przygotowawcze

Wyczyścić wszystkie reguły zapory przygotowane w p. 2

```
#wyczyszczenie wszystkich poprzednich reguł
iptables -F
iptables -X
#ustalenie domyślnych polityk
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
```

Zainstalować aplikację fail2ban

```
apt-get update
apt-get install fail2ban
```

3.3. Zadania

Zainstalować aplikację fail2ban

Skonfigurować ochronę systemu przed klientami wywołującymi 3 nieudane próby logowania do usługi SSH.

Skonfigurować ochronę systemu przed klientami odwołującymi się do nieistniejących adresów WWW.

Sprawdzić skuteczność blokad.

Sprawdzić nowe reguły wprowadzone dynamicznie do zapory sieciowej.

```
iptables -nvL
```