S I E C I K O M P U T E R O W E I

LABORATORIUM NR 10
Zapory sieciowe

Celem ćwiczenia jest zapoznania się z programową zaporą sieciową systemu Linux IPTABLES oraz wykorzystanie jej możliwości do rozwiązania postawionych problemów w typowej sieci LAN.

Informacje wstępne:

Zapora sieciowa zawiera filtr pakietów, którego zadaniem jest sprawdzanie nagłówków pakietów przepływających przez stos protokołów. Decyduje o ich losie, akceptując (ang. ACCEPT) lub odrzucając (ang. DROP) poszczególne pakiety.

Konfigurowanie filtracji polega na definiowaniu tzw. reguł (ang. rule). Pojedyncza reguła składa się z wzorca i akcji. Gdy wiadomość poddawana jest analizie, najpierw dopasowywana jest do wzorca; jeśli do niego pasuje, o dalszym losie wiadomości decyduje akcja reguły. Jeśli zaś dane w wiadomości nie pasują do wzorca danej reguły, pod uwagę brana jest kolejna reguła.

UWAGA: Reguły przeglądane są w takim porządku, w jakim zostały wprowadzone.

Dla danego pakietu przeszukiwanie reguł trwa do momentu pierwszego dopasowania do wzorca lub (w przypadku braku dopasowania) do wyczerpania reguł.

Akcja reguły zależy od jej typu. Wyróżnia się trzy typy reguł:

- *reguły filtrujące,*
- *reguły translacji NAT,*
- *reguły do manipulacji zaawansowanymi opcjami protokołu IP.*

W trakcie ćwiczenia wykorzystywane są głównie reguły filtrujące i reguły translacji. W przypadku tych pierwszych typową akcją jest odrzucenie (DROP) lub akceptacja wiadomości (ACCEPT). Wszystkie reguły tego samego typu pamiętane są w strukturze zwanej tablicą (ang. table), od której pakiet bierze swą nazwę. Istnieją trzy wbudowane tablice:

- *filter (dla reguł filtrujących),*

• *nat (dla reguł translacji NAT),*

• *mangle (dla reguł manipulujących opcjami IP).*

Na każdym etapie można stosować do danego pakietu różne typy reguł. Dlatego wewnątrz każdej tablicy reguły są dodatkowo grupowane ze względu na etap przetwarzania pakietu. Sekwencja reguł powstała przez połączenie tych grup nazywa się łańcuchem (ang. chain).

Wykorzystywany w trakcie ćwiczenia pakiet iptables zawiera pięć wbudowanych łańcuchów:

• *INPUT (dla datagramów pierwszego rodzaju),*

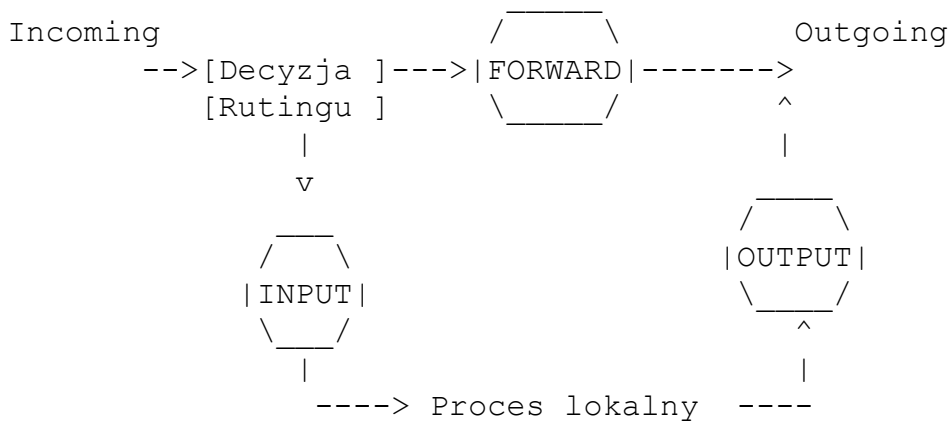
• *OUTPUT (dla pakietów drugiego rodzaju),*

• *FORWARD (dla pakietów rutowanych)*

• *PREROUTING (tylko w tablicach nat i mangle),*

• *POSTROUTING (tylko w tablicach nat i mangle)*

Najprostszy związek pomiędzy łańcuchami w pakiecie Iptables ilustruje rysunek poniżej:



Trzy okręgi reprezentują trzy łańcuchy, o których wspomniano wyżej. Kiedy pakiet dociera do danego okręgu na diagramie, sprawdzany jest łańcuch reguł by zdecydować o losie pakietu. Jeśli łańcuch mówi, że należy odrzucić (DROP) pakiet, jest on odrzucany tutaj, ale jeśli łańcuch mówi by zaakceptować pakiet (ACCEPT), kontynuuje on swoją podróż po diagramie.

UWAGA: Łańcuch to lista reguł. Każda reguła mówi 'jeśli nagłówek pakietu wygląda tak, to zrobimy z tym pakietem następującą rzecz'. Jeśli reguła nie pasuje do pakietu, sprawdzana jest następna. Na koniec, jeśli nie ma więcej reguł, kernel sprawdza domyślną politykę (ang. policy) danego łańcucha. W systemie w którym dba się o bezpieczeństwo, polityka mówi zwykle kernelowi by odrzucić (DROP) pakiet.

Przykładowo, kiedy pakiet dociera do hosta (np. kartę ethernetową), sprawdzany najpierw jest adres IP przeznaczenia pakietu i realizowany jest proces routingu. Jeśli pakiet przeznaczony jest do tego hosta to zostaje on przepuszczony do łańcucha INPUT. Zawarte tam reguły decyduj ą czy otrzyma go proces lokalny, do którego był adresowany.

UWAGA: Jeśli kernel nie ma włączonego przekazywania pakietów IP (ang. forwarding), lub nie wie jak przekazać pakiet, jest on odrzucany.

Jeśli przekazywanie jest włączone i pakiet jest przeznaczony do innego interfejsu sieciowego, pakiet przechodzi do łańcucha FORWARD. Jeśli zostaje zaakceptowany (ACCEPT), zostanie wysłany dalej. Na koniec, proces lokalny działający na hoście może również wysyłać własne pakiety. Przejdą one od razu do łańcucha OUTPUT. Jeśli według reguł zawartych w tym łańcuchu zostaną one zaakceptowane (ACCEPT), pakiety wysłane zostaną do właściwego interfejsu sieciowego.

Używanie Iptables:

Program *iptables* ma bardzo szczegółowy podręcznik (*man iptables*), do którego warto zajrzeć zawsze gdy pojawiają się wątpliwości co do sposobu jego wykorzystania.

Ogólna postać reguły:
iptables [-t tablica] komenda [wzorzec] [akcja]

Komendy:

- -P łańcuch polityka - ustawienie domyślnej polityki dla łańcucha. Domyślna polityka stosowana jest dopiero wówczas, gdy pakiet nie pasuje do żadnej reguły łańcucha,
- -A łańcuch - dodanie reguły do określonego łańcucha,
- -I łańcuch [nr reguły] – wstawienie reguły do określonego łańcucha, jeśli zostanie podany nr reguły wtedy reguła zostanie wpisane w to miejsce zmieniając kolejność pozostałych,
- -L [łańcuch] – wyświetlenie wszystkich reguł łańcucha (lub wszystkich łańcuchów w danej tablicy); często używane z opcjami -n i -v,
- -F [łańcuch] – usunięcie wszystkich reguł łańcucha (lub ze wszystkich łańcuchów danej tablicy),
- -D łańcuch [nr reguły] – usunięcie konkretnej reguły w określonym łańcuchu, jeśli zostanie podany nr reguły wtedy zostanie usunięta reguła o tym numerze,
- -R łańcuch nr_reguły – zastąpienie reguły numer w określonym łańcuchu.

Opcje wzorca:

- -s [!] ip[/netmask] – adres IP źródłowy (może być uogólniony do adresu sieci),
- -d [!] ip[/netmask] – adres IP docelowy (może być uogólniony do adresu sieci),
- -p [!] protokół – wybór protokołu: tcp, udp lub all (wszystkie protokoły stosu TCP/IP),
- -i [!] interfejs wejściowy
- -o [!] interfejs wyjściowy
- --sport [!] port:[port] – port źródłowy,
- --dport [!] port:[port] – port docelowy,
- -m moduł – załadowanie modułu rozszerzającego, dzięki temu można wykorzystać kolejne opcje danego modułu.

Najważniejsze akcje:

- -j ACCEPT – przepuszczenie dopasowanych pakietów,
- -j DROP – usunięcie dopasowanych pakietów,
- -j REJECT – odrzucenie dopasowanych pakietów,
- -j LOG – logowanie dopasowanych pakietów, bez usunięcia ich z łańcucha,
- -j RETURN – usunięcie pakietu z łańcucha, pozwalając jednocześnie, aby dalej był pakiet sprawdzany w kolejnych łańcuchach,
- -j SNAT – translacja adresów źródłowych,
- -j DNAT – translacja adresów docelowych,
- -j SAME – translacja adresów źródłowych i docelowych,
- -j REDIRECT – przekierowanie pakietów do lokalnego systemu,
- -j MASQUERADE – translacja adresów źródłowych na adres dynamicznie przyznawany na interfejsie.

PRZYKŁADY:

Ustawienie domyślnej polityki łańcucha INPUT na DROP:

iptables -P INPUT DROP

Akceptacja pakietów o adresie źródłowym 150.254.20.20:
iptables -A INPUT -s 150.254.20.20 -j ACCEPT

Translacja adresów źródłowych dla podsieci 192.168.1.0/24 na adres 150.254.20.20
iptables -t nat -I PREROUTING -s 192.168.1.0/24 -j SNAT –- to 150.254.20.20

Translacja adresów docelowych z 150.254.20.21 na 192.168.1.2:
iptables -t nat -A POSTROUTING -d 150.254.20.21 -j DNAT –-to 192.168.1.2

Translacja adresów źródłowych na zakres adresów:
iptables -t nat -A PREROUTING -s 192.168.1.0/24 -j SNAT --to 150.254.20.20 – 150.254.20.30

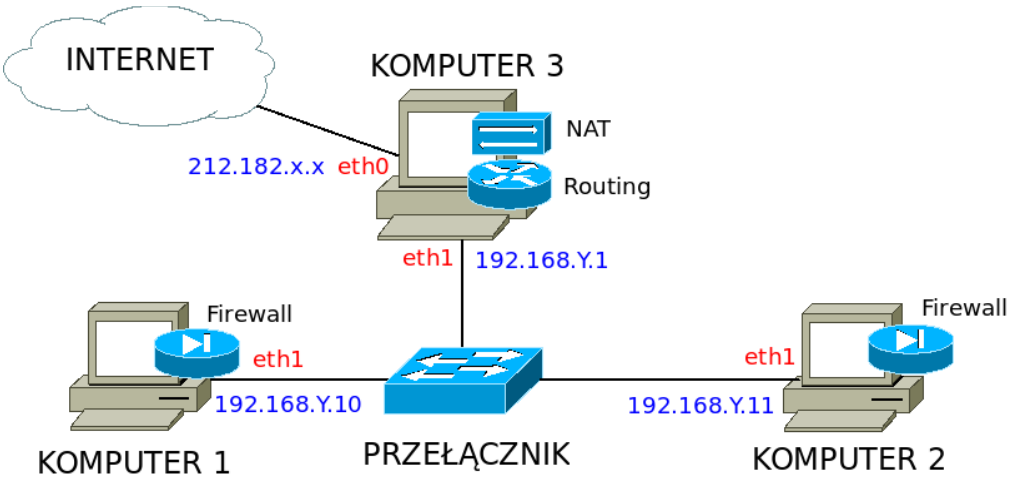
Translacja adresów i portów docelowych, jedynie dla wybranego portów:
iptables -t nat -A POSTROUTING -p tcp -d 150.254.20.21 –-dport 80 -j DNAT –to 192.168.1.3:8080

Przebieg ćwiczenia:

Do wykonanie zadań niezbędne będą uprawnienia root-a.
Należy również deaktywować Network Managera na wszystkich trzech komputerach
Przed połączeniem komputerów w docelową konfigurację i wyłączeniem Network Managera należy:

- na komputerze 3 zainstalować program *nmap*. Proszę użyć polecenie:
sudo apt-get install nmap

- na komputerze 1 zainstalować pakiet *openssh*. Proszę użyć polecenie:
sudo apt-get install openssh-server



W trakcie ćwiczenia wszystkie komputery należące do poszczególnych grup ćwiczeniowych tworzyć będą jedną sieć połączoną do wybranego przełącznika sieciowego poprzez sieć laboratoryjną (LAN). Komputer pełniący rolę bramy sieciowej ma mieć dwie aktywne karty sieciowe, pierwszą przyłączoną do sieci LAN a drugą do obwodu sieciowego INTERNET. Topologię sieci przedstawia rysunek poniżej. Instrukcje podłączenia przedstawi prowadzący.

Zadanie 1. Ustawienie podstawowej polityki filtrowania pakietów.

a. Należy wyłączyć na wszystkich komputerach Network Manager. Następnie należy przypisać adresy sieciowe interfejsom komputerów przyłączonych ze switchem (zgodnie z rysunkiem wyżej). Interfejs eth0 (przyłączony do Internetu) powinien otrzymać adres publiczny z serwera DHCP. (polecenie sudo dhclient eth0). Po wykonaniu tych zadań, proszę sprawdzić połączenie pomiędzy komputerami (polecenie ping)

b. Na wszystkich komputerach należy sprawdzić obecne ustawienia zapory sieciowej za pomocą polecenia
sudo iptables -L lub sudo iptables -nL

c. W celu wyczyszczenia ustawień iptables na każdym komputerze należy wydać polecenia:

```
student@cloudlab:~$ sudo iptables -F
student@cloudlab:~$ sudo iptables --table nat --flush
student@cloudlab:~$ sudo iptables --delete-chain
student@cloudlab:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
student@cloudlab:~$
```

Wykonanie polecenia sudo iptables -L powinno dać wynik jak wyżej.

Zadanie 2. Ustawienie prostej polityki filtrowania pakietów.

a. Ustawienie podstawowych reguł otrzymywania ruchu sieciowego na komputerach 1 oraz 2:
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

b. Zezwolenie na przyjmowanie ruchu sieciowego na port 22 (ssh)
sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT

c. Zezwolenie na przyjmowanie ruchu sieciowego na port 80 (http)
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

W sprawozdaniu proszę umieścić otrzymaną konfigurację iptables na jednym z hostów.

d. Na komputerze 3 należy wydać polecenie sprawdzające stan portów na komputerach 1 i 2:
nmap -sT *adres_IP*
gdzie zamiast *adres_IP* proszę wstawić kolejno adresy IP komputerów 1 oraz 2.

e. W sprawozdaniu należy umieścić wynik działania tego polecenie dla obu komputerów. Jeśli rezultaty różnią się pomiędzy sobą to proszę podać przyczynę.

f. W jakich stanach mogą znajdować się porty monitorowane za pomocą programu nmap. (jakie stany może wyświetlić polecenie z podpunktu d) ?

g. Jakie opcje –state odnoszące się do połączeń TCP można podać w module state pakietu iptables i co one oznaczają (przykład użycia modułu state podany był w podpunkcie a) ?

Zadanie 3. Blokowanie ruchu.

Po zezwoleniu na określone rodzaje transmisji, typowo pozostały ruch należy zablokować.

a. Proszę sprawdzić czy polecenie ping pomiędzy komputerami 1 i 2 kończy się sukcesem. Jeśli tak, można przejść do polecenia blokującego pozostały ruch:
sudo iptables -A INPUT -j DROP

W sprawozdaniu proszę umieścić otrzymaną konfigurację iptables dla komputera 1 albo 2.
Czy polecenie ping pomiędzy komputerem 1 i 2 kończy się sukcesem.

b. Należy określić polecenie, które pozwoli na ponowne działanie polecenia ping. Proszę pamiętać, ze kolejność reguł w łańcuchu ma znaczenie.

c. W sprawozdaniu proszę umieścić: użyte polecenie zezwalające na korzystanie z ping, konfigurację iptables po wykonanej modyfikacji oraz zrzut ekrany działania polecenia ping pomiedzy komputerem 1 a 2.

Zadanie 4. Translacja adresów sieciowych NAT na komputerze 3

a. Należy włączyć przekazywanie pakietów (wymagane zalogowanie jako root):
echo 1 > /proc/sys/net/ipv4/ip_forward

b. Uruchomienie translacji NAT (masquerading):
sudo iptables –t nat -A POSTROUTING -o eth0 -j MASQUERADE

Czy możliwe jest pingowanie dowolnego adresu publicznego (np. serwera WWW) z komputerów 1 lub 2 ? W sprawozdaniu proszę umieścić konfigurację iptables po poprawnym uruchomieniu NAT

c. Dotychczasowa konfiguracja komputerów 1 oraz 2 nie pozwala na dostęp do stron WWW w Internecie. Proszę zaproponować modyfikację firewalla na komputerach 1 i 2, która przywróci możliwość korzystania z usług opartych o protokoły TCP/HTTP. Czy trzeba coś zmienić w konfiguracji komputera 3 ? W sprawozdaniu proszę umieścić użyte polecenie/polecenia zezwalające na dostęp do stron WWW oraz konfigurację iptables na wszystkich komputerach, na których dokonano modyfikacji.

c. Jeżeli istnieje konieczność uruchomienia serwera za NAT-em to konieczne jest skorzystanie z możliwości przekazywania portów. Załóżmy, że serwer WWW zainstalowano na komputerze 2 i nasłuchuje on na porcie 8080. Jak powinno wyglądać polecenie przekazujące (forwardujące) ruch przychodzący na port 80 do komputera 3 na port 8080 na komputerze 2.
W sprawozdaniu proszę umieścić: użyte polecenie zezwalające na poprawne przekazywanie portu 80 oraz konfigurację iptables po wykonanej modyfikacji.

!!!
1. Sprawozdanie należy nazwać "Cw10-nazwisko" gdzie nazwisko, oznacza nazwisko wykonującego sprawozdanie i wgrać do katalogu na Dropbox (katalog Sprawozdania, podkatalog odpowiadający terminowi zajęć).
2. Na wstępie sprawozdania proszę podać imiona i nazwiska wszystkich członków grupy ćwiczeniowej, która uczestniczyła w wykonaniu ćwiczenia.
3. Format sprawozdania: PDF. !
!!!