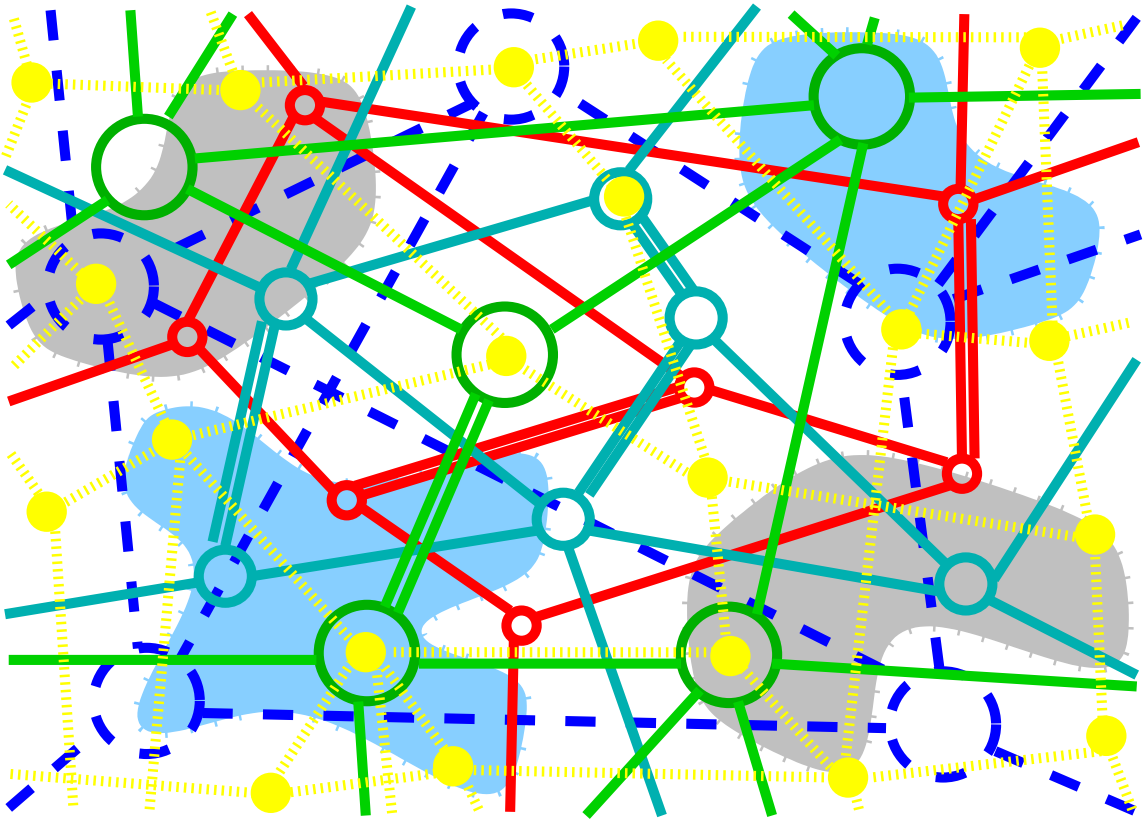
Instrukcja do laboratorium sieci komputerowych

Ściana ogniowa

dr inż. Piotr Arabas **mgr inż. Jerzy Sobczyk** **dr inż. Edward Śliwa**



30 lipca 2024

6 Ćwiczenie 6 Ściana ogniowa

6.1 Przygotowanie do zajęć

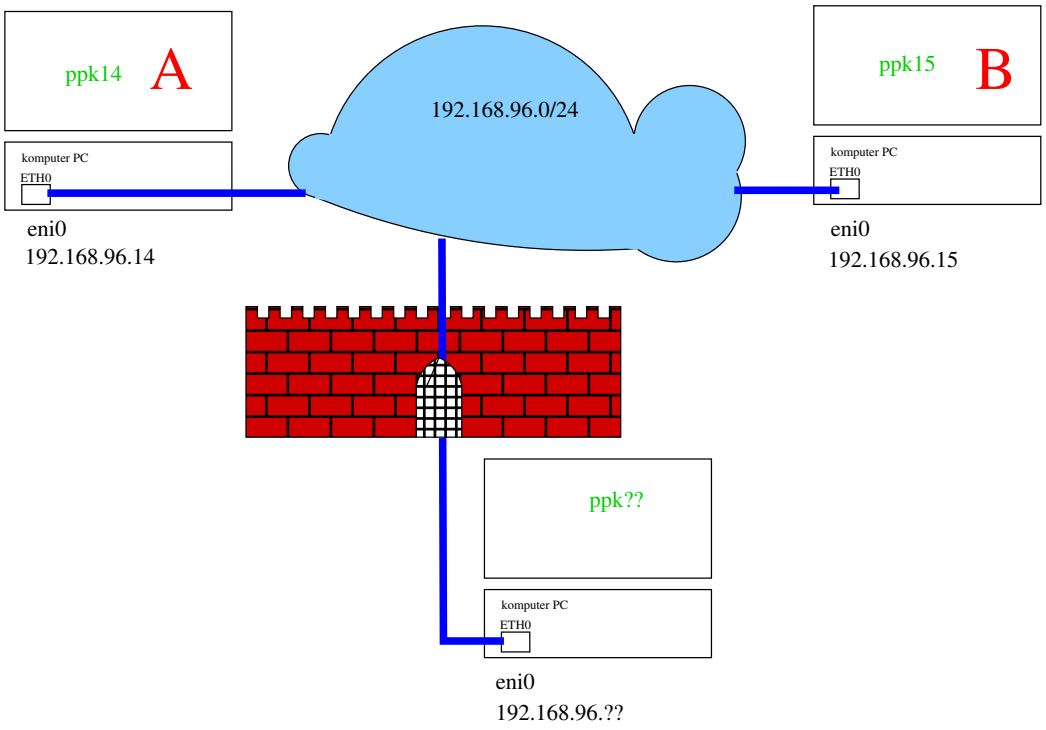
1. W czasie wykonywania ćwiczenia niezbędna będzie wiedza z zakresu następujących tematów:
   - protokół IP (adresowanie)
   - protokół TCP (adresowanie, mechanizm nawiązywania połączenia)
   - translacja adresów sieciowych (NAT – translacja portów)
2. Przed przystąpieniem do ćwiczenia należy zapoznać się z opisem (np. instrukcje dostępne w sieci www) programów wykorzystywanych w ćwiczeniu, w szczególności:
   - **iptables** - w zakresie konfiguracji z linii komendy oraz poprzez plik administracyjny
   - **nft** - w zakresie konfiguracji z linii komendy oraz poprzez plik administracyjny (opcjonalnie)
   - standardowe sieciowe narzędzia diagnostyczne i administracyjne (`ipconfig`/`ip`, `route`, `netstat`, `ping`)

6.2 Logowanie do stanowiska roboczego

- W czasie ćwiczenia niezbędne będzie korzystanie z trzech komputerów:
  - *stanowiska roboczego* – komputera znajdującego się w s 327, na którym będą konfigurowane reguły zapory sieciowej,
  - komputerów `ppk14.ise.pw.edu.pl` oraz `ppk15.ise.pw.edu.pl`, które w ćwiczeniu będą służyć jako komputery testujące działanie wprowadzonych reguł; w dalszej części instrukcji komputery te będą nazywane odpowiednio: *komputerem testującym A* i *komputerem testującym* B.
- Zalogować się na stanowisku roboczym. Większość komend używanych w ćwiczeniu wymaga uprawnień administratora systemu – dlatego należy zalogować się jako użytkownik `ppkroot`. Hasło zostanie podane w czasie ćwiczenia.
- Zalogować się (przez `ssh`) na komputery testujące `ppk14.ise.pw.edu.pl` oraz `ppk15.ise.pw.edu.pl`.
- Sprawdzić parametry interfejsu sieciowego stanowiska roboczego i komputerów testujących.
- W sprawozdaniu zamieścić dane (nazwy, adresy MAC i numery IP) stanowiska roboczego i komputerów testujących.

6.3 Ograniczanie dostępu do stanowiska roboczego (filtracja pakietów w warstwie sieciowej)

1. Przed kolejnymi punktami należy sprawdzić stan reguł filtra pakietów i w razie potrzeby usunąć wszystkie reguły.
2. Blokada dostępu dla niepożądanego hosta.
   - Skonfigurować filtr pakietów w taki sposób, by zablokować wszelki dostęp do stanowiska roboczego dla stacji testującej A, zachowując swobodny dostęp dla innych komputerów.
   - Sprawdzić działanie wprowadzonych reguł poprzez komendę `ping` oraz próby próby nawiązania połączenia TCP z komputerów testujących A i B.
3. Blokada dostępu dla niepożądanego hosta z umożliwieniem sprawdzenia, czy stanowisko robocze działa.
   - Skonfigurować filtr pakietów analogicznie jak w poprzednim punkcie, ale umożliwiając wszystkim komputerom w sieci sprawdzenie działania stanowiska roboczego za pomocą komendy `ping`.



Rysunek 8: Schemat połączeń ćwiczenia 6

- Sprawdzić działanie wprowadzonych reguł poprzez komendę `ping` oraz próby próby nawiązania połączenia TCP z komputerów testujących A i B.

4. Umożliwienie dostępu tylko dla wybranego hosta.

   - Skonfigurować filtr pakietów w taki sposób, by umożliwić dostęp do stanowiska roboczego tylko dla stacji testującej B, blokując dostęp dla innych komputerów, ale z zachowaniem możliwości sprawdzenie działania stanowiska roboczego za pomocą komendy `ping`.
   - Sprawdzić działanie wprowadzonych reguł poprzez komendę `ping` oraz próby próby nawiązania połączenia TCP z komputerów testujących A i B.

5. Ukrywanie obecności stanowiska roboczego w sieci (*security by obscurity*).

   - Skonfigurować filtr pakietów w taki sposób, by umożliwić dostęp do usług sieciowych TCP stanowiska roboczego dla innych komputerów, ale z zablokowaniem możliwości sprawdzenia działania stanowiska roboczego za pomocą komendy `ping` dla wszystkich hostów poza komputerem testującym B.
   - Sprawdzić działanie wprowadzonych reguł poprzez komendę `ping` oraz próby próby nawiązania połączenia TCP z komputerów testujących A i B.

6. Uwagi.

   - Wprowadzania i ewentualnych modyfikacji reguł filtra pakietów należy dokonywać z linii komendy.
   - Wykonanie poszczególnych punktów ćwiczenia należy udokumentować w sprawozdaniu poprzez:
     - zamieszczenie użytych do konfiguracji komend,
     - zamieszczenie wyników testów.
   - Do sprawdzenia wyników próby nawiązania połączenia TCP należy użyć usługi `DAYTIME` i/lub `SSH`.

6.4 Ograniczanie dostępu do usług sieciowych (filtracja pakietów w warstwie transportowej)

1. Przed kolejnymi punktami należy sprawdzić stan reguł filtra pakietów i w razie potrzeby usunąć wszystkie reguły.
2. Umożliwienie dostępu do wybranych usług sieciowych.
   - Skonfigurować filtr pakietów w taki sposób, by umożliwić dostęp do stanowiska roboczego tylko dla dwóch usług sieciowych: `DAYTIME` oraz `SSH`.
     Należy zachować możliwość sprawdzenia działania stanowiska roboczego za pomocą komendy `ping`.
   - Sprawdzić działanie wprowadzonych reguł poprzez komendę `ping` oraz próby próby nawiązania odpowiednich połączeń TCP z komputera testującego.
3. Blokada dostępu do wybranych usług sieciowych dla niepożądanego hosta.
   - W konfiguracji z poprzedniego punktu wprowadzić dodatkową regułę pozwalającą zablokować dostęp do usługi `ssh` dla hosta A.
   - Sprawdzić działanie wprowadzonych reguł poprzez próby próby nawiązania połączenia TCP z komputerów testujących A i B.
4. Umożliwienie dostępu do wybranych usług sieciowych ze zmianą numeru portu.
   - Dla filtra pakietów skonfigurowanego jak w punkcie 2 wprowadzić modyfikację pozwalającą na dostęp do usługi `ssh` tylko na niestandardowym porcie 2222.
   - Sprawdzić działanie wprowadzonych reguł poprzez próby próby nawiązania odpowiednich połączeń TCP z komputera testującego.
5. Automatyczna konfiguracja reguł zapory.
   - Reguły umożliwiające automatyczną konfigurację filtra pakietów z punktu 2 należy zamieścić w pliku `/usr/local/etc/active`). Plik ten jest wykorzystywany do określania reguł zapory w momencie startu komputera, i w momencie rozpoczęcia ćwiczenia nie powinien zawierać reguł ograniczających ruch sieciowy.
   - Wykonać restart systemu i sprawdzić konfigurację filtra pakietów po restarcie.
6. Uwagi.
   - Wprowadzania i ewentualnych modyfikacji reguł filtra pakietów należy dokonywać z linii komendy
   - Wykonanie poszczególnych punktów ćwiczenia należy udokumentować w sprawozdaniu poprzez:
     - zamieszczenie użytych do konfiguracji komend,
     - zamieszczenie wyników testów,
     - zamieszczenie zawartości odpowiednich plików konfiguracyjnych.

6.5 Sprawozdanie z wykonania ćwiczenia

- Z wykonania ćwiczenia należy przygotować sprawozdanie w postaci pliku .pdf.
- Sprawozdanie należy zamieścić na serwerze `studia`.

6.6 Uwagi

- Ćwiczenie wykonywane jest jednoosobowo.
- Przy określaniu adresów warstwy sieciowej można używać zarówno numerów IP (w notacji kropkowo-dziesiętnej) jak i nazw symbolicznych – prostych (jednoczłonowych) i domenowych (wieloczłonowych).
- Przy określaniu adresów warstwy transportowej można używać zarówno numerów portów w postaci liczbowej jak i nazw symbolicznych. Odpowiednie odwzorowania można znaleźć w pliku `/etc/services`.
- Należy zwrócić uwagę, że np. zablokowanie dostępu do stacji roboczej (np. w p.6.3) nie oznacza blokady w drugą stronę – stacja robocza powinna nadal mieć dostęp do hostów, które blokuje, i sprawdzenie tego należy zamieścić w sprawozdaniu (por. uwaga poniżej).
- W niektórych sytuacjach adresy źródłowe lub docelowe mogą nie być znane z góry. Dla przykładu, w protokole TCP jeden port będzie numerem portu dynamicznego/efemerycznego – czyli numerem losowo generowanym przez system operacyjny. Aby poprawnie odbierać od odpowiedzi na pakiety z takim adresem źródłowym filtr pakietów musi zapamiętać odpowiedni numer przy wysyłaniu pakietu do serwera usługi sieciowej. Obsługę sekwencji tego typu pakietów zapewnia rozszerzenie programu `iptables` o moduł ***`conntrack`*** (moduł ten jest standardowo dostępny w programie `iptables`. Zapoznanie się ze składnią i opcjami tego modułu pozostawiamy wykonującym ćwiczenie, w ramach przygotowania do zajęć.
  Oprócz protokołów warstwy transportowej, moduł ten może okazać się przydatny przy filtracji odpowiedzi na pakiety ICMP.

6.7 Pożyteczne komendy i ich opcje

Do konfiguracji reguł filtra pakietów można używać:

- historycznie starszej komendy `iptables` – z punktu widzenia ćwiczenia jest to prostsze rozwiązanie,
- nowszej komendy `nft` – jest to rozwiązanie bardziej złożone, ale w kolejnych wersjach systemu Linux przewiduje się stopniową rezygnację z komendy `iptables`.

Wybór sposobu konfiguracji należy do wykonującego ćwiczenie.

W dalszej części tego punktu zostaną krótko opisane podstawowe opcje komendy `iptables`, mogą być one jednak niewystarczające do wykonania ćwiczenia – studenci przed wykonaniem ćwiczenia zapoznać się z dokumentacją tej komendy.

Oznaczenia używane w opisach:	
tbl	Tabela. Możliwe wartości: `filter`, `nat`, `mangle`, `raw`. W ćwiczeniu będą wykorzystywane tylko tabele `filter` i `nat`.
chn	Łańcuch. Możliwe wartości: `INPUT`, `OUTPUT` i `FORWARD` dla tabeli `filter`, `PREROUTING`, `OUTPUT` i `POSTROUTING` dla tabeli `nat`. W ćwiczeniu tylko niektóre z tych łańcuchów będą wykorzystywane.
nr	Numer reguły w łańcuchu.
tgt	Przeznaczenie pakietu. Wykorzystywane w ćwiczeniu wartości tego parametru to: `ACCEPT` i `DROP` (w tabeli `filter`) oraz `REDIRECT` (w tabeli `nat`).
prot	Protokół. Możliwe wartości: `tcp`, `udp`, `icmp`.
addr	Adres IP w postaci: *a.b.c.d* lub *a.b.c.d/m*, gdzie *a, b, c, d* są liczbami z zakresu 0-255, *m* jest liczbą jedynek w masce sieci.

6.7.1 `iptables`

Podstawowe opcje przydatne w ćwiczeniu to:	
`-t` ***tbl***	Tabela, której dotyczy reguła. Ominięcie tej opcji spowoduje przyjęcie tabeli `filter` jako domyślnej.
`-L` [***chn***]	Wyświetlenie listy reguł w łańcuchu ***chn*** (lub we wszystkich łańcuchach danej tabeli w przypadku ominięcia parametru ***chn***).
`-F` [***chn***]	Usunięcie wszystkich reguł z łańcucha ***chn*** (lub ze wszystkich łańcuchów danej tabeli w przypadku ominięcia parametru ***chn***). Uwaga! Polecenie to **nie zmienia** domyślnej polityki łańcucha.
`-A` ***chn***	Wstawienie reguły na końcu łańcucha ***chn***.
`-I` ***chn nr***	Wstawienie reguły w pozycji ***nr*** w łańcuchu ***chn***. Ominięcie parametru ***nr*** jest równoznaczne z przyjęciem wartości 1.
`-D` ***chn nr***	Usunięcie pozycji o numerze ***nr*** z łańcucha ***chn***. Zamiast numeru reguły można też podać pełną specyfikację usuwanej reguły.
`-P` ***chn tgt***	Ustawienie domyślnej polityki: akceptacja (`ACCEPT`) lub usunięcie (`DROP`).
W określeniu samych reguł przydatne mogą być następujące opcje:	
`-p` ***prot***	Protokół, którego dotyczy reguła.
`-s` ***addr***	Adres źródłowy datagramu.
`-d` ***addr***	Adres docelowy datagramu.
`-j` ***tgt***	Określenie przeznaczenia pakietu: akceptacja (`ACCEPT`) lub usunięcie (`DROP`).

6.7.2 `nft`

Zapoznanie się ze składnią komendy `nft` pozostawiamy jako samodzielne zadanie w ramach przygotowania do zajęć.