Ćwiczenie 08a Konfigurowanie i testowanie zapór sieciowych (na przykładzie *Windows Firewall*)

Celem ćwiczenia jest zapoznanie studentów z przykładową procedurą definiowania i testowania reguł osobistej zapory sieciowej. Realizowane zadania obejmują definiowanie reguł, których celem jest ograniczanie ruchu do/z komputera a następnie testowanie poprawności pracy zapory. W czasie ćwiczeń należy wykorzystywać protokół IPv4 (ICMPv4).

W ramach przygotowania do ćwiczenia należy zapoznać się z udostępnionymi materiałami wykładowymi.

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie według załączonego wzoru, zawierające obrazy odpowiednich okien, oraz wnioski i komentarze dotyczące realizowanych zadań.

Przed przystąpieniem do ćwiczenia należy wyłączyć rolę *Remote Access* wraz z funkcją *Routing* – jeżeli nie zrobiono tego na zakończenie poprzednich ćwiczeń. Jeżeli udostępniane są jakiekolwiek folder, to należy zakończyć ich udostępnianie. Nie dotyczu to folderów udostępnianych automatycznie np. C$, IPC$ itp.

Ćwiczenie 8.1 Definiowanie filtra aplikacji *Interner Explorer*

1. Zalogować się jako administrator.
2. W oknie zarządcy serwera (*Server Manager)* wybrać pozycję serwera lokalnego (*Local Server)*. Opcja zwiększonych zabezpieczeń przeglądarki Internet Explorer (*IE Enhanced Security Configuration*) powinna być wyłączona dla wszystkich użytkowników (*Administrators* oraz *Users*).
3. W oknie zarządcy serwera (*Server Manager)* uaktywnić usługę zapory sieciowej (*Windows Firewall*). W konsoli zapory sieciowej Windows (*Windows Firewall*) należy wybrać przycisk ustawień rekomendowanych (*Use recommended settings)*. Przejść do zaawansowanych ustawień zapory sieciowej (*Advanced settings*). Zapoznać się z regułami dla połączeń wchodzących (*Inbound Rules*) i połączeń wychodzących (*Outbound Rules*). Czy widnieje tam pozycja odpowiadająca programowi ***Internet Explorer***? Zminimalizować okno *Windows Firewall with Advanced Security*.
4. Uruchomić ***Internet Explorer*** i dokonać próby połączenia z witryną *http://www.wp.pl* a następnie z witryną uczelni.
5. Przywrócić okno *Windows Firewall with Advanced Security* przejść do zakładki połączeń wychodzących (*Outbound Rules)*, następnie wybrać przycisk umożliwiający tworzenie nowej reguły (*New Rule*). W oknie tworzenia nowej reguły (*New Outbound Rule Wizard)* wybrać opcję *Custom*. W kolejnym oknie zaznaczyć opcję *This program path* i wskazać ścieżkę do programu ***Internet Explorer***. Należy zwrócić uwagę, że program o tej nazwie występuje zarówno w folderze ***Program Files*** jak i w folderze ***Program Files(x86)***. W kolejnym oknie w polu typu protokołu (*Protocol type)* wybrać opcję TCP, a w polu zdalnego portu (*Remote port*) wpisać wartość *80*. W kolejnym oknie, w polu określania adresu zdalnego (*Which remote IP address does this rule apply to?)* dodać *(Add)* adres uczelnianego serwera WWW i zatwierdzić zmiany. W oknie definiowania akcji (*Action*) zaznaczyć opcję blokowania połączenia (*Block the connecion)*. W kolejnym oknie (*Profile*) zostawić ustawienia domyślne. W oknie nazwy (*Name*) wpisać nazwę dla utworzonej reguły IE_xxx (gdzie xxx jest identyfikatorem studenta realizującego ćwiczenie) i zakończyć definiowanie reguły (*Finish)*.

6. Dokonać próby nawiązania połączenia z witryną Uczelni, a następnie z witryną *http://www.wp.pl*. Która próba zakończyła się powodzeniem i dlaczego?
7. Zmodyfikować zdefiniowaną poprzednio regułę tak aby oprócz witryny Uczelni, zablokowane były połączenia z witryną *http://www.sejm.gov.pl*.
8. Sprawdzić działanie reguły poprzez próby połączeń z witrynami: *www.sejm.gov.pl, www.onet.pl, www.wp.pl* i witryną Uczelni. Które próby zakończyły się powodzeniem i dlaczego?

Ćwiczenie 8.2 Definiowanie reguł zaawansowanych

1. W oknie *Windows Firewall with Advanced Security* wyłączyć wszystkie reguły zapory sieciowej dla połączeń wychodzących (*Outbound Rules*) i przychodzących (*Inbound Rules*). W tym celu po zaznaczeniu reguł, w menu akcji (*Action*) należy wybrać funkcję wyłączenia (*Disable Rule*).
2. Dokonać skanowania (*ping)* swojego komputera.
3. Dlaczego nie odpowiada na pakiety *ICMP Echo Request*?
4. Zdefiniować regułę dla połączeń przychodzących (*Inbound Rules*) pozwalającą odpowiadać na pakiety *ICMP Echo Request* (tylko i wyłącznie) przysyłane z dowolnego komputera. Regule nadać nazwę PING_xxx (gdzie xxx jest identyfikatorem studenta realizującego ćwiczenie).
5. Sprawdzić działanie – tak skonfigurowana zapora powinna teraz zezwolić na odpowiadanie na pakiety *ICMP Echo Request*. W razie niepowodzenia, poprawić regułę.
6. W menu podręcznym korzenia konsoli zarządzania zaporą sieciową (*Windows Firewall with Advanced Security on Local Computer)* wybrać pozycję właściwości (*Properties*).
7. Dla każdej ze stref (*Domain Profile, Private Profile, Public Profile*) wybrać przycisk *Customize* odnoszący się do funkcji rejestrowania (*Logging)*. Sprawdzić domyślną lokalizację dla pliku dziennika. Włączyć logowanie odrzuconych pakietów (*Log dropped packets)* oraz połączeń zakończonych sukcesem (*Log successful connecions)*. Zatwierdzić zmiany. Zamknąć okno *Windows Firewall with Advanced Security*
8. Po wyłączeniu zapory, wyczyścić dziennik zapory poprzez skasowanie pliku dziennika a następnie ponownie włączyć zaporę.
9. Dokonać skanowania (*ping*) własnego komputera (z innego hosta) oraz dokonać próby połączenia się z nim na portach (135÷139, 445), np. poprzez podłączenie do udostępnionego foldera (C$). Można wykorzystać polecenie ***net use***. Przed przejściem do kolejnego zadania odczekać około 30 sekund.
10. Skopiować plik dziennika ruchu na pulpit nadając mu nazwę PFIREWALL_xxx.csv (gdzie xxx jest identyfikatorem studenta realizującego ćwiczenie). Przy pomocy programu notatnika sprawdzić zawartość tego pliku.
11. Dokonać edycji tego pliku usuwając w 4 linii od góry tekst: *#Fields*, pamiętając o tym, żeby nie zostawiać spacji na początku wiersza, zapisać zmiany. Sprawdzić jaki znak jest wykorzystywany jako separator kolumn.
12. Otworzyć plik PFIREWALL_xxx.csv przy pomocy programu ***OpenOffice Calc*** *(*dwuklik). W otwartym oknie importu jako separator wskazać znak spacji (*Space*).
13. Uszeregować kolumny raportu w kolejności: ***date, time, action, protocol, src-ip, src-port, dst-ip, dst-port,*** pozostałe bez znaczenia. Odnaleźć i zaznaczyć zapisy związane z próbami przeprowadzonymi w punkcie 9 niniejszego zadania.

Ćwiczenie 8.3 Sterowanie dostępem do komputera

1. Wyczyścić dziennik zapory.
2. Utworzyć folder o nazwie LAB_08_xxx (gdzie xxx jest identyfikatorem studenta realizującego ćwiczenie) i udostępnić go pod tą samą nazwą.
3. Ponownie otworzyć okno *Windows Firewall with Advanced Security.* Odświeżyć obraz reguł zapory sieciowej dla połączeń wychodzących (*Outbound Rules*) i przychodzących (*Inbound Rules*). Należy zauważyć, że mimo wcześniejszego wyłączenia wszystkich reguł, po udostępnieniu folderu, system Windows automatycznie aktywował stosowne reguły.
4. Dokonać próby podłączenia się do udostępnionego udziału LAB_08_xxx.
5. Dokonać importu pliku dziennika (patrz ćwiczenie 8.2) do programu ***OpenOffice Calc*** Przejrzeć wpisy w dzienniku. Uszeregować kolumny raportu w kolejności: ***date, time, action, protocol, src-ip, src-port, dst-ip, dst-port***, pozostałe bez znaczenia. Zaznaczyć zielonym kolorem wpisy dotyczące próby podłączenia się do udostępnionego zasobu.
6. W kontenerze reguł zapory sieciowej dla połączeń przychodzących (*Inbound Rules*) deaktywować reguły: *File and Printer Sharing (SMB-In)* oraz *File and Printer Sharing (NB-Session-In)*. Zapoznać się z definicjami obu reguł. Zwrócić zwłaszcza uwagę na opis (*Description*) i numery portów (*Local Port*).
7. Korzystając z konsoli zarządzania komputerem (*Computer Management*) zamknąć otwarte sesje *NetBIOS* i ponownie dokonać próby podłączenia się do udostępnionego zasobu (tak jak w zadaniu 4). Funkcja zamykania sesji dostępna jest po wybraniu podkontenera sesji (*Sessions*) w kontenerze udostępnianych udziałów (*Shared Folders*).
8. Dokonać importu pliku dziennika do programu ***OpenOffice Calc*** Przejrzeć wpisy w dzienniku. Uszeregować kolumny raportu w kolejności: ***date, time, action, protocol, src-ip, src-port, dst-ip, dst-port***, pozostałe bez znaczenia. Dokonać sortowania w sposób pozwalający na zgrupowanie zapisów spowodowanych przeprowadzoną próbą podłączenia. Zaznaczyć czerwonym kolorem wpisy dotyczące próby podłączenia się do udostępnionego zasobu.
9. Wprowadzić regułę o nazwie SMB_NEIGHBOR_XXX_yyy (gdzie xxx jest identyfikatorem studenta realizującego ćwiczenie, a yyy jest identyfikatorem wybranego partnera), która umożliwiać będzie tylko temu jednemu, wybranemu partnerowi dostęp do zasobów Twojego komputera, przy wykorzystaniu protokołu SMB. Sprawdzić i udokumentować w sprawozdaniu poprawność działania reguły.

Ćwiczenie 8.4 Definiowanie reguł zapory sieciowej z poziomu programu *PowerShell*

1. Otworzyć okno programu ***PowerShell***.
2. Wyświetlić stan zapory sieciowej Windows przy pomocy następującego polecenia, uruchamianego w oknie programu ***PowerShell***:

```
Get-NetFirewallProfile
```

3. Przywrócić ustawienia fabryczne zapory sieciowej Windows przy pomocy następujących poleceń, uruchamianych w oknie programu ***PowerShell***:

```
$fw=New-Object  -ComObject  HNetCfg.FwMgr
$fw.RestoreDefaults()
```

4. Przy pomocy polecenia uruchamianego w oknie programu ***PowerShell*** zdefiniować nową regułę, która będzie powodowała blokowanie połączeń inicjowanych przez przeglądarkę

Internet Explorer (w miejscu elementów zaznaczonych niebieskim kolorem należy wpisać odpowiednie wartości rzeczywiste - xxx jest identyfikatorem studenta realizującego ćwiczenie)

```
New-NetFirewallRule -Program "C:\Program Files(x86)\Internet Explorer\iexplore.exe"
-Action Block -Profile Domain, Private, Public -DisplayName "Blokowanie_xxx"
-Description "imię i nazwisko studenta" -Direction Outbound
```

Sprawdzić czy definicja reguły pojawiła się w konsoli *Windows Firewall with Advanced Security*.
Sprawdzić funkcjonowanie zdefiniowanej reguły.

5. Przy pomocy polecenia uruchamianego w oknie programu ***PowerShell,*** ograniczyć blokowanie połączeń przez ***Internet Explorer*** tylko do witryny *www.wp.pl* (w miejscu elementów zaznaczonych niebieskim kolorem należy wpisać odpowiednie wartości rzeczywiste)

```
Set-NetFirewallRule -DisplayName "Blokowanie_xxx" -RemoteAddress adres_www.wp.pl
-Protocol TCP -RemotePort 80 -LocalAddress adres_IP_komputera_ćwiczącego
```

Sprawdzić czy definicja reguły pojawiła się w konsoli *Windows Firewall with Advanced Security*.
Sprawdzić funkcjonowanie zmodyfikowanej reguły.

6. Wyłączyć zaporę sieciową Windows.