Ćwiczenie 07a Konfigurowanie i testowanie kanałów *IPSec*

Celem ćwiczenia jest zapoznanie studentów z przykładową procedurą tworzenia i testowania kanału IPSec w systemie Windows. Realizowane zadania obejmują skonfigurowanie kanału IPSec pomiędzy dwoma komputerami partnerskimi a następnie testowanie poprawności pracy utworzonego kanału. W czasie testowania studenci „podglądają" przy pomocy snifera ruch sieciowy w takim kanale i porównują go z ruchem sieciowym pomiędzy komputerami w przypadku, gdy kanał IPSec nie został skonfigurowany lub zabezpieczenia zostały wyłączone.

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 protokół IPv6. W czasie realizacji ćwiczenia należy użyć snifera *Wireshark.*

Zadanie 1 Weryfikacja poprawności komunikacji

1. Jeżeli wcześniej został zainstalowany pakiet PGP lub GPG, to należy go teraz „*odinstalować*".
2. Według wskazówek prowadzącego, skonfigurować protokół TCP/IP (v.4)na obu komputerach, na których realizowane będzie ćwiczenie. Jeżeli wskazówki nie zostaną przekazane, to do konfigurowania interfejsów sieciowych należy wykorzystać usługę DHCP. Komputery te umownie będą oznaczone w dalszym opisie ćwiczenia jako A i B.
3. Na obu komputerach, w oknie programu ***PowerShell*** uruchomić program ***mmc*** i do utworzonej konsoli dodać przystawkę monitorującą zabezpieczenia IP (*IP Security Monitor)*. Zapisać plik konsoli na pulpicie pod nazwą **MONITOR_IPSEC**_xxx (gdzie xxx jest identyfikatorem studenta). W konsoli **MONITOR_IPSEC**_xxx otworzyć okno właściwości swojego komputera i ustawić czas odświeżania na 20 sekund.
4. Wykorzystując program ***ping***, na obu komputerach sprawdzić poprawność komunikacji z komputerem partnera. Obserwować jednocześnie zawartość okna snifera i kontenerów statystyka *(statistic)* w konsoli **MONITOR_IPSEC**_xxx dla trybu głównego *(main mode)* i szybkiego *(quick mode).* Co i dlaczego prezentowane jest w wymienionych oknach?

Zadanie 2 Konfigurowanie kanału IPSec.

Ćwiczenie to powinno zostać zrealizowane na obu komputerach partnerskich.

Do konsoli **MONITOR_IPSEC**_xxx dodać przystawkę służącą do zarządzania zasadami zabezpieczeń IP (*IP Security Policy Management).* Przystawka ta ma umożliwiać zarządzanie usługą na komputerze lokalnym

Zbudować zasadę reguł komunikacji IPSec:

1. W oknie konsoli, w menu podręcznym pozycji określającej zasady zabezpieczeń IP na lokalnym komputerze (*IP Security Policies on Local Machine)* wybrać funkcję tworzenia zasady zabezpieczeń IP *(Create IP Security Policy).*
2. Korzystając z uruchomionego kreatora, nadać konstruowanej zasadzie nazwę **ZASADA_IPSEC_**xxx, (gdzie xxx jest identyfikatorem studenta). W trakcie pracy kreatora wyczyścić opcję włączającą regułę domyślnej odpowiedzi (*Activate the default response rule*), oraz edytującą właściwosci (*Edit properties)*.

Zdefiniować reguły sterujące ruchem:

1. Otworzyć okno właściwości zasady **ZASADA_IPSEC_**xxx.
2. W oknie zakładki reguł *(Rules)* wyczyścić pole wyboru udostępniające kreatora dodawania (*Use Add Wizard),* a następnie wybrać przycisk dodający *(Add)* nową regułę.
3. W oknie zakładki z listą filtrów IP (*IP Filter List)* wybrać przycisk dodawania filtra *(Add).*
4. W oknie z listą filtrów IP (*IP Filter List)* wyczyścić pole wyboru udostępniające kreatora dodawania (*Use Add Wizard).* W polu nazwy wpisać: **DO**_*nazwa.komputera.partnera_xxx* (gdzie xxx jest identyfikatorem studenta)*,* a następnie wybrać przycisk tworzący nowy filtr *(Add)*.
5. W oknie zakładki z adresami (*Adresses*), w polu adresu źródłowego wybrać opcję ustalającą własny adres IP (*My IP Address).* W polu adresu docelowego wybrać opcję umożliwiającą określenie konkretnego adresu IP (*A specific IP Address)* i podać adres komputera partnera. Zastanowić się, jakie znaczenie mają pozostałe opcje i kiedy się ich używa. Wyczyścić opcję udostepniającą dublowanie (*Mirrored),* by reguła nie dotyczyła pakietów przesyłanych z komputera partnera do naszego komputera.
6. W oknie zakładki specyfikującej typ protokołu (*Protocol)* wybrać dowolny *(Any).*
7. W oknie zakładki z opisem (*Description*), wprowadzić opis zgodny z nawą filtra: **DO**_*nazwa.komputera.partnera_xxx* (gdzie xxx jest identyfikatorem studenta). Zatwierdzić wszystkie wprowadzone ustawienia*.*
8. W oknie zakładki z listą filtrów IP (*IP Filter List)* zaznaczyć pozycję filtra **DO**_*nazwa.komputera.partnera_xxx* (gdzie xxx jest identyfikatorem studenta).
9. Wybrać zakładkę zawierającą ustawienia tunelowania (*Tunnel Settings)* i w jej oknie zakreślić pole wyboru wskazujące, że dana reguła nie specyfikuje tunelu IPSec.
10. Wybrać zakładkę z akcją filtrowania (*Filter Action)* i w jej oknie wyczyścić pole wyboru udostepniające kreatora dodawania (*Use Add Wizard),* a następnie wybrać przycisk definiujący akcję filtra *(Add)*.
11. W konfiguracji nowego filtra pozostawić aktywną opcję ustalającą negocjowanie protokołu zabezpieczeń (*Negotiate Security)* i zakreślić opcję wymuszającą akceptowanie komunikacji niezabezpieczonej przy jednoczesnej odpowiedzi z użyciem IPSec (*Accept unsecured communication, but always respond using IPSec).*
12. Wybrać przycisk dodaj *(Add)* i w kolejnym oknie dialogowym zaznaczyć opcję integralności i szyfrowania *(Integrity and encryption)***.** Zatwierdzić zmiany powracając do okna zakładki z akcją filtrowania (*Filter Action).*
13. W oknie zakładki zawierającej metody uwierzytelnienia (*Authentication Method)* należy wybrać metodę uwierzytelnienia przy zastosowaniu klucza wstępnego (*Preshared key)* i wpisać ustalone z partnerem hasło. Wybrana metoda powinna być jedyną w liście wybieranych metod.

14. Samodzielnie zdefiniować regułę umożliwiającą przekazywanie danych w drugą stronę i nadać jej nazwę **DO**_*nazwa.komputera.własnego_xxx* (gdzie xxx jest identyfikatorem studenta. Dla tej reguły należy przyjąć inne hasło niż dla reguły zdefiniowanej wcześniej.

Należy pamiętać, że każda reguła (filtr) określa sposób komunikowania się w jedną stronę. W związku z tym bardzo ważne jest np. rozróżnienie początku i końca kanału. Przemyśl to i podaj odpowiednie wartości w polach, które wypełniałeś realizując niniejsze ćwiczenia, a teraz musisz te same pola wypełnić samodzielnie.

Aktywować zdefiniowaną zasadę ZASADA_IPSEC_XXX wybierając w jej menu podręcznym (okno główne konsoli) odpowiednią pozycję (*Assign).*

Zadanie 3 Testowanie poprawności pracy kanału IPSec.

1. Zrestartować zbieranie pakietów w programie snifera**.** Na komputerze A, wykorzystując okno wiersza poleceń i program ***ping*** sprawdzić poprawność komunikacji z komputerem B. Program ***ping*** uruchomić dwukrotnie w odstępach około pół minuty. Jednocześnie obserwować zawartość okien snifera i kontenerów ze statystykami *(Statistics)* w konsoli **MONITOR_IPSEC**_xxx dla trybu głównego *(main)* i szybkiego *(quick)*.
2. Dokonać deaktywacji zdefiniowanych na obu komputerach zasad **ZASADA_IPSEC**_xxx wybierając w ich menu podręcznym (okno główne konsoli) odpowiednią pozycję (*Un-assign).*
3. Dokonać aktywacji zdefiniowanych na obu komputerach zasad **ZASADA_IPSEC**_xxx wybierając w ich menu podręcznym (okno główne konsoli) właściwą pozycję *(Assign).*
4. Zrestartować zbieranie pakietów w programie snifera**.** Na komputerze B, wykorzystując okno wiersza poleceń i program ***ping*** sprawdzić poprawność komunikacji z komputerem A. Program ***ping*** uruchomić dwukrotnie w odstępach około pół minuty. Jednocześnie obserwować zawartość okien programu snifera i kontenerów ze statystykami *(Statistics)* w konsoli **MONITOR_IPSEC**_xxx dla trybu głównego *(main)* i szybkiego *(quick)*.

Zadanie 4 Wyłączanie zabezpieczeń IPSec.

1. Na komputerze A dokonać deaktywacji zdefiniowanej zasady wybierając w jej menu podręcznym (okno główne konsoli) odpowiednią pozycję (*Un-assign)*.
2. Przy pomocy programu ***ping*** sprawdzić poprawność komunikacji na obu komputerach. Jednocześnie obserwować zawartość okien programu snifera i kontenerów ze statystykami *(Statistics)* w konsoli **MONITOR_IPSEC**_xxx dla trybu głównego *(main)* i szybkiego *(quick)*.
3. Na komputerze A dokonać aktywacji zdefiniowanej zasady wybierając w jej menu podręcznym (okno główne konsoli) właściwą pozycję *(Assign)*.
4. Przy pomocy programu ***ping*** sprawdzić poprawność komunikacji na obu komputerach. Jednocześnie obserwować zawartość okien programu snifera i kontenerów ze statystykami *(Statistics)* w konsoli **MONITOR_IPSEC**_xxx dla trybu głównego *(main)* i szybkiego *(quick)*.
5. Dokonać deaktywacji zdefiniowanych na obu komputerach zasad **ZASADA_IPSEC**_xxx wybierając w ich menu podręcznym (okno główne konsoli) odpowiednią pozycję (*Un-assign)*. Usunąć wyżej wymienione zasady. Zatrzymać na obu komputerach zbieranie pakietów w programie snifera. Na obu komputerach, w oknie wiersza poleceń wydać

polecenie ***net stop policyagent***.

6. Skasować konsolę **MONITOR_IPSEC_XXX**.