Bezpieczeństwo systemów rozproszonych

SPRAWOZDANIE Z ĆWICZENIA: Komunikacja sieciowa w MS Windows

Imię Nazwisko: ..... nr albumu: .....

data ćwiczenia: ..... godzina: .....

1. Otoczenie sieciowe MS Windows

Zadanie przygotowawcze:

Upewnij się, że twoje stanowisko (system wirtualny) posiada unikalną nazwę, po której można będzie je zidentyfikować w otoczeniu sieciowym.

Zweryfikuj zdalną widoczność zasobów maszyny wirtualnej w otoczeniu sieciowym. Jakie protokoły i usługi są odpowiedzialne za tę widoczność?

1.1 Udziały sieciowe

1. Utwórz i udostępnij w sieci katalog C:\PUBLIC. Jakie uprawnienia zdalnego dostępu zostały domyślnie przydzielone?

2. Zezwól na zdalny dostęp do tego katalogu w trybie do zapisu dla wybranego użytkownika. Zweryfikuj ten dostęp.

3. Czy możliwy jest dostęp dowolnego uwierzytelnionego użytkownika w sieci (w domenie) bez określania jego nazwy? Grupa o jakiej nazwie reprezentuje takich użytkowników:

1.2 Udziały domyślne

4. Usuń udziały domyślne swojego stanowiska komputerowego. Zweryfikuj rezultat. Jakiego polecenia należy użyć do weryfikacji?

1.3 Połączenia sieciowe

5. Sprawdź listę aktywnych połączeń TCP w systemie.
   Co to za połączenia? Opisz 2 z nich (port < 1024):

   1:

   2:

2. Zapora sieciowa Windows

6. Za pomocą zapory Windows zablokuj możliwość dostępu do serwisu `www.facebook.com` z wybranej przeglądarki (np. Edge). Przetestuj czy zastosowane rozwiązanie nie blokuje ruchu dla innych aplikacji (np. Firefox).
7. Zablokuj możliwość pingowania swojego systemu z sąsiedniego komputera (tylko!), pozostawiając sobie możliwość pingowania innych. Następnie podaj odpowiednie polecenie netsh:
8. Spróbuj zablokować ping na pętli zwrotnej. Zweryfikuj i wytłumacz rezultat:

2.2 Monitorowanie pracy zapory

9. Aktywuj i przetestuj rejestrowanie odrzuconych pakietów. Gdzie znajduje się utworzony log?

10. W dzienniku systemowym znajdź zdarzenia związane ze zmianą konfiguracji zapory systemowej. Podaj przykładowe typy zdarzeń, które tam zawarte.

11. Utwórz filtr pozwalający na przeglądanie zdarzeń zgłoszonych przez zaporę systemu Windows związanych z dodaniem aplikacji (składnika Windows) do domyślnej listy reguł.