Bezpieczeństwo systemów informatycznych

SPRAWOZDANIE Z ĆWICZENIA: Komunikacja sieciowa w MS Windows

Imię Nazwisko: ..... nr albumu: .....

data ćwiczenia: ..... godzina: .....

1. Sieć

Zadanie przygotowawcze:

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

1.1 Otoczenie sieciowe

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

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

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

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

1.1.2 Udziały

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

1.2 Ukrycie komputera w otoczeniu sieciowym

6. Sprawdź widoczność swojego stanowiska w otoczeniu sieciowym. Przetestuj ukrywanie jego nazwy. Czy cały czas możliwe jest korzystanie z udostępnianych zasobów?

1.3 Połączenia sieciowe

7. Sprawdź listę aktywnych połączeń TCP w systemie. Co to za połączenia? (opisz co najmniej 4 z nich)

1:

2:

3:

4:

1.4 Zapory sieciowe

8. Za pomocą wbudowanej zapory systemu Windows zablokuj możliwość dostępu do serwisu `www.facebook.com` z poziomu przeglądarki Firefox. Przetestuj czy zastosowane rozwiązanie nie blokuje ruchu dla innych aplikacji (np. Internet Explorer).

9. Za pomocą wbudowanej zapory systemu Windows zablokuj całkowicie komunikację z wykorzystaniem protokołu ICMP. Przetestuj konfigurację za pomocą polecenia `ping`. Co istotnego należało zrobić aby osiągnąć cel? Podaj uzasadnienie.

10. Aktywuj rejestrowanie połączeń odrzuconych i przetestuj działanie. Gdzie znajduje się utworzony log? Jakie informacje można z niego uzyskać?

11. Skonfiguruj zaporę systemu Windows w taki sposób, aby umożliwiała dostęp komputerom z zewnątrz do serwera uruchomionego lokalnie na porcie 9876. Co należy zrobić w tym celu?

12. Skonfiguruj zaporę systemu Windows w taki sposób, aby umożliwiała dostęp do aplikacji `ncat` niezależnie od numeru portu, na którym ta zostanie uruchomiona. Co należy zrobić w tym celu?

1.5 Podgląd zdarzeń

13. W logu systemowym znajdź zdarzenia związane ze zmianą konfiguracji zapory systemowej. Podaj przykładowe typy zdarzeń, które tam zawarte. Jak sądzisz, dlaczego są one zapisywane w logu?

14. Utwórz filtr pozwalający na przeglądanie zdarzeń zgłoszonych przez zaporę systemu Windows związanych z dodaniem reguły do listy wyjątków. W jaki sposób można to uzyskać?