Bezpieczeństwo systemów rozproszonych

SPRAWOZDANIE Z ĆWICZENIA: Komunikacja sieciowa w MS Windows

Imię Nazwisko: Dariusz Max Adamski ..... nr albumu: 136674 .....

data ćwiczenia: 15.12.2020 ..... godzina: 15:10 .....

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?

NetBIOS, SMB

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

Po wejsciu w Properties -> Sharing -> Share folderu Public (jako Administrator) domyslnie sa przydzielone uprawnienia:
Administrators: Owner
Administrator: Read/Write
(Wedlug skryptu powinny byc tez Everyone: Read, ale ja musialem dodac to sam)

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:

Everyone

1.1.2 Udziały

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

net share

1.2 Połączenia sieciowe

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

1: Po otwarciu wikipedii nawiazane jest polaczenie z 91.198.174.208 (serwer fundacji wikimedia) na porcie 443, czyli z usluga HTTPS (HTTP po TLS/SSL).

2: Podczas przegladania internetu nawiazane zostalo polaczenie z 92.123.189.138 (serwer akamai) na porcie 80, czyli z usluga HTTP.

1.3 Zapory sieciowe

7. Za pomocą wbudowanej zapory systemu Windows zablokuj możliwość dostępu do serwisu `www.facebook.com` z przeglądarki Internet Explorer. Przetestuj czy zastosowane rozwiązanie nie blokuje ruchu dla innych aplikacji (np. Firefox).
8. Zablokuj możliwość pingowania swojego systemu z sąsiedniego komputera (tylko!), pozostawiając sobie możliwość pingowania innych. Następnie podaj odpowiednie polecenie netsh:

netsh advfirewall firewall add rule name="Neighbor ICMPv4" protocol=icmpv4:any,any dir=in interface=any action=block remoteip=X.X.X.X

Gdzie X.X.X.X to adres IP sasiedniego komputera

9. Spróbuj zablokować ping na pętli zwrotnej. Zweryfikuj i wytłumacz rezultat:

Ping nadal dziala. Windows Firewall nie pozwala na zablokowanie komunikacji na petli zwrotnej.

10. Skonfiguruj zaporę systemu Windows w taki sposób, aby umożliwiała dostęp do aplikacji netcat niezależnie od numeru portu, na którym ta zostanie uruchomiona.

11. Skonfiguruj zaporę systemu Windows w taki sposób, aby umożliwiała dostęp do serwera uruchomionego na porcie 9876.
12. Aktywuj rejestrowanie połączeń odrzuconych i przetestuj działanie.
    Gdzie znajduje się utworzony log?

    %systemroot%\System32\LogFiles\Firewall\pfirewall.log

1.4 Podgląd zdarzeń

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

    Zmiana ustawien (dodanie/usuniecie reguly)
    Odrzucone polaczenie (jesli rejestrujemy)
    Zaakceptowane polaczenie (jesli rejestrujemy)

14. Utwórz filtr pozwalający na przeglądanie zdarzeń zgłoszonych przez zaporę systemu Windows związanych z dodaniem reguły do listy wyjątków.