

Wnioski z ćwiczenia – CW30

WNIOSKI Z ĆWICZENIA: Sieci wirtualne VPN – narzędzia dostępu zdalnego WS 2019

1. Uczniowie zrozumieli pełny proces konfiguracji środowiska VPN w oparciu o Windows Server 2019 i Windows 11, obejmujący przygotowanie interfejsów sieciowych, konfigurację DNS oraz poprawne przypisanie ról serwerowych.
2. W trakcie ćwiczenia wykazano, że poprawna konfiguracja RRAS (Routing and Remote Access) umożliwia realizację usług VPN oraz NAT, co pozwala klientom VPN korzystać z zasobów sieci lokalnej oraz z Internetu przez tunel VPN.
3. Analiza połączeń VPN wykazała znaczenie protokołów PPTP/MPPE, a także potwierdziła działanie tunelu, przypisywanie adresów PPP oraz poprawny przepływ ruchu między klientem a serwerem.
4. Badanie ruchu sieciowego w Wireshark pozwoliło uczniom rozpoznać pakiety związane z tunelowaniem, szyfrowaniem i translacją adresów, co wzmacnia ich umiejętność diagnozowania połączeń VPN.
5. Analiza tabeli mapowania sesji NAT wykazała działanie mechanizmu PAT, który umożliwia jednocześnie zestawienie wielu połączeń wychodzących z jednego adresu publicznego.
6. Przetestowanie polityki NRPT (Name Resolution Policy Table) potwierdziło, że zapytania DNS dla domeny szkolnej kierowane są tunelem VPN do serwera domenowego, co zapobiega wyciekom DNS.
7. Uczniowie wykonali pomyślnie dołączenie komputera klienckiego do domeny przez tunel VPN, co wymagało poprawnego skonfigurowania metryki interfejsów, DNS oraz odpowiednich ustawień połączenia systemowego.
8. Ćwiczenie potwierdziło, że kontrola dostępu oparta na kontach domenowych i zasadach NPS pozwala precyzyjnie definiować użytkowników uprawnionych do korzystania z VPN.
9. Całość zadania umożliwiła kompleksowe opanowanie zagadnień związanych z konfiguracją, analizą i zabezpieczaniem sieci VPN w środowisku Windows Server 2019.
10. Uczniowie nabyli praktyczne kompetencje związane z diagnozowaniem problemów poprzez polecenia ping, ipconfig, nslookup oraz analizę dzienników i narzędzi sieciowych.