Instalacja i wstępna konfiguracja Windows Server 2025
Cele zajęć (dla ucznia)

- wykonuje podstawową konfigurację serwera,
- konfiguruje role: **AD DS, DNS, DHCP**,
- zakłada użytkowników i jednostki organizacyjne,
- testuje poprawność działania usług.

Wymagania wstępne

- Znajomość podstaw Windows 10/11,
- Konto lokalnego administratora.

Instalacja systemu Windows Server
1: Przygotowanie maszyny wirtualnej
Polecenia:

1. Utwórz nową maszynę wirtualną:
    - Typ: Microsoft Windows
    - Wersja: Windows Server 2025 (64-bit)
2. Przydziel:
    - RAM: min. 2048 MB
    - CPU: 1-2 rdzenie
    - Dysk: 40 GB (dynamiczny)
3. Podłącz plik ISO Windows Server 2025.

2: Instalacja Windows Server

1. Uruchom instalator.
2. Wybierz wersję:
    - **Windows Server 2025 Standard (Desktop Experience)**.
3. Typ instalacji: **Custom**.
4. Utwórz jedną partycję systemową.
5. Ustaw hasło administratora zgodnie z zasadami bezpieczeństwa. (***Poszukaj w sieci aktualnych rekomendacji na temat bezpiecznych haseł i uzasadnij w trakcie oceny powołując się na wiarygodne źródła.***)

3: Konfiguracja podstawowa (Server Manager)

1. Otwórz **Server Manager**.
2. Zmień:
    - Nazwę komputera na: `SERV-AD`
    - Strefę czasową na `(UTC+01:00) Warszawa`
3. Skonfiguruj kartę sieciową:
    - IP: `192.168.1.10`
    - Maska: `255.255.255.0`
    - Brama: `192.168.1.1`
    - DNS: `127.0.0.1`

4: Aktualizacje i zabezpieczenia

1. Sprawdź dostępność aktualizacji Windows Update.
2. Włącz:
    - Zapora Windows Defender
3. Sprawdź status:
    - Windows Defender
    - Windows Update

Konta, hasła i polityki bezpieczeństwa

Wprowadzenie

- Czym jest hardening
- Najczęstsze błędy adminów (konto Administrator, brak GPO, brak audytu)

5 : Zabezpieczenie kont

1. Zmień nazwę konta **Administrator**:
    - np. `AdSRV`
2. Utwórz nowe konto administracyjne:
    - `SecurityAd`
3. Odbierz uprawnienia administratora zwykłym użytkownikom.

✔ Efekt: brak domyślnego konta admina.

6: Polityka haseł (GPO)

1. Otwórz **Group Policy Management**
2. Edytuj **DefaultDomain Policy**
3. Ustaw:
    - min. długość hasła: **10 do 15 znaków**
    - złożoność: **włączona**
    - historia haseł: **5**
    - blokada konta po **5 błędnych logowaniach**

✔ Efekt: silne hasła i ochrona przed brute-force.

Zasady logowania i audyt

7: Ograniczenie logowania administratorów

1. W GPO ustaw:
    - Zakaz logowania lokalnego dla zwykłych użytkowników
    - Logowanie lokalne tylko dla administratorów
2. Ogranicz logowanie RDP:
    - tylko grupa `Administratorzy`

8: Audyt zdarzeń

1. W GPO włącz audyt:
    - logowania
    - zmiany kont
    - zmiany GPO
2. Sprawdź **Event Viewer → Security** **`(eventvwr.msc)`**

✔ Efekt: możliwość śledzenia działań użytkowników.

Usługi, zapora i protokoły

9: Wyłączanie zbędnych usług

1. Otwórz **Services.msc**
2. Zidentyfikuj i wyłącz (jeśli nieużywane):
    - PrintSpooler.
    - Fax
    - Remote Registry**.**
3. Ustaw tryb: Disabled

✔ Efekt: zmniejszona powierzchnia ataku.

Aktualizacje, kopie zapasowe i testy

10: Windows Update

1. Skonfiguruj automatyczne aktualizacje

2. Sprawdź historię aktualizacji

11: Kopia zapasowa

1. Zainstaluj **Windows Server Backup**
2. Wykonaj:
    - kopię stanu systemu (System State)
3. Wskaż lokalizację kopii

✔ Efekt: możliwość odtworzenia AD.

12: Windows Defender i Firewall

1. Sprawdź:
    - Real-timeprotection
2. Skonfiguruj zaporę:
    - Zezwól tylko na:
        - DNS
        - LDAP
        - DHCP
        - RDP (ograniczone)
3. Zablokuj wszystkie inne połączenia przychodzące.

13: Test hardeningu

1. Przetestuj:
    - blokadę konta po błędnych logowaniach
    - dostęp RDP z konta ucznia
2. Sprawdź logi zdarzeń
3. Sporządź krótką listę wdrożonych zabezpieczeń.