Muntlig-praktisk oppgave 2024

Veiledning

Oppgaven består av to deler. Du skal løse og fremføre oppgaven individuelt. Du må gjerne bruke PowerPoint eller lignende i presentasjonen din, men du skal også vise resultatet av ditt arbeid i VMer i skolens datasenter. Merk: Presentasjonen din skal *ikke* være en steg-for-steg-guide for hvordan oppgaven løses. Du har 20 minutter til rådighet for fremførelsen.

Del 1

Det har vært en rekke cyberangrep mot bedriften Flomservice AS den siste tiden. For ekstra sikring ønsker IT-avdelingen et servermiljø med mindre angrepsflate. De har fire serverroller som dette gjelder: en domenekontroller med domene, en DHCP-server, en DNS-server og en HyperV-server. De ønsker ikke at administrative oppgaver skal utføres fysisk på disse serverne.

Del 2

Du skal hjelpe Flomservice AS med domenestrukturen i bedriften. Bedriften har 14 ansatte. Ved hjelp av PowerShell skal du opprette brukere, grupper og en velorganisert OU-struktur som skal kunne håndtere fremtidige GPOer på en tydelig og effektiv måte. Under fremførelsen av oppgaven din bør du kunne demonstrere opprettelsen av en bruker, gruppe og OU med PowerShell.

Dette er Flomservice AS:

Sjef:

- Bjørn Strøm - Daglig leder Øvrig ledelse:
- Vera Foss - Økonomisjef
- Lars Elvheim - HR-sjef
- Ingrid Vannvik - Driftsleder IT-avdeling:
- Erik Dammen - IT-sjef
- Sofia Bru - Systemadministrator

Classification: Confidential (V3)

Flomarbeidere:

- Ola Flo
- Anders Elvebakken
- Petter Fossvik
- Siri Vassli
- Even Tjern
- Mona Holme

Revisorer:

- Steinar Riedal
- Maria Fjellbekk

Disse bruker en rekke datamaskiner, bestående av laptoper:

- LenovoThinkPad T14s
- DellVostro 3520, • HPProBook 450 G9 … og stasjonære:

- Dell OptiPlex 7020
- HP ProDesk 400 G9 Mini
- Lenovo ThinkCentre M80s G3

Løsning

For å løse oppgaven for Flomservice AS, her er en løsning jeg tror kan løse både del 1 og del 2, med fokus på sikkerhet, organisering og bruk av PowerShell.

Del 1: Servermiljø for redusert angrepsflate

Målet vårt i del 1 er å opprette et sikrere servermiljø som inkluderer en domenekontroller, DHCP-server, DNS-server og Hyper-V-server.

Viktig ting vi kan tenke på her:

- Server Core
- Domene kontroller,
- DHCP
- DNS
- Hyper-V settes i core men lette i GUI)

For administrering kan man bruke:

- Enter-PSSession (PowerShell)
- PAW (Privileged access workstation)
- WAC (Windows Admin Center)

Servermiljøet:

- Her burde vi implementere en dedikert Admin-stasjon:

Begrensning av tilganger:

- Her kan vi opprette egne administrasjonskontoer som kun har nødvendig tilgangsnivå til hver server. Her kan vi tenke på de ulike administrative rollene i selskapet.
- Bruke gruppepolicyer (GPOer) til å håndheve sikkerhetsinnstillinger:
- f.eks
    - to-faktor-autentisering for administratorer
    - begrensede privilegier.

Nettverksisolering

- Vi kan plassere hver serverrolle i et isolert nettverkssegment for å begrense mulighetene for angrep.

Bruk av Hyper-V:

- Vi kan bruke Hyper-V-serveren til å virtualisere de andre serverrollene. Dette vil da gi oss fleksibilitet for å ta backups og gjøre hele prosessen enklere.

Oppdateringer:

- Vi kan sette opp rutiner for regelmessig patching og oppdatering av serverne.

Del 2: Opprette en domenestruktur med PowerShell

Her er målet vårt å bygge en effektiv og tydelig OU-struktur for å håndtere brukere, grupper og fremtidige GPOer.
Her er noen notater før vi begynner med selve oppgaven.

Powershell CLI for brukere New-ADUser -Name "Test Bruker" -Path "OU=FlomService,DC=Flomservice,DC=AS"

For OU-er New-ADOrganizationalUnit -Name "Test OU" -Path "OU=FlomService,DC=Flomservice,DC=AS"

For Groups New-ADGroup -Name "Test Bruker" -Path "OU=FlomService,DC=Flomservice,DC=AS" -GroupScope Global -GroupCategory Security

Her er strukturen vi kan føle:

- FlomserviceAS
  - Ledelse
    - Daglig Leder
    - Økonomi
    - HR
    - Drift
  - IT-Avdeling
    - IT-Sjef
    - Systemadministrator
  - Flomarbeidere
  - Revisorer

Vi har allerede skrevet en del kommandoer oppe som notater, men her er det en mer detaljert prosess

1. Opprette en OU:
   - **New-ADOrganizationalUnit -Name "Ledelse" -Path "OU=FlomserviceAS,DC=flomservice,DC=local"**

2. Opprettelse av brukere (For eksempel, opprett Bjørn Strøm som daglig leder.)
   - **New-ADUser -Name "Bjørn Strøm" -GivenName "Bjørn" -Surname "Strøm" -SamAccountName "bjorn.strom" -UserPrincipalName "bjorn.strom@flomservice.local" -Path "OU=Daglig Leder,OU=Ledelse,OU=FlomserviceAS,DC=flomservice,DC=local" -AccountPassword (ConvertTo-SecureString "Pass@ord123" -AsPlainText -Force) -Enabled $true**

3. Opprettelse av grupper (For eksempel, opprett en gruppe for økonomiavdelingen)
   - **New-AD Group -Name "Økonomi" -SamAccountName "Okonomi" -GroupCategory Security -GroupScope Global -Path "OU=Ledelse,OU=FlomserviceAS,DC=flomservice,DC=local"**

4. Legge til en bruker på en gruppe:
   - **Add-ADGroupMember -Identity "Okonomi" -Members "vera.foss"**

5. Automatiseringsprosess for alle ansatte:

For å effektivisere hele prosessen kan vi bruke en PowerShell-skript-fil som oppretter alle brukere og grupper i en loop.