PRBIT – Tasks Windows 2022 – Windows 1 – Tasks for students

Task 1 - creating a local user

Evaluation: 0.5 b

Getting to know the Windows Server environment.

Resources:

- Default groups: https://ss64.com/nt/syntax-security_groups.html
- Net command: https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/net-commands-on-operating-systems

Tasks marked with * need to be solved via command line / PowerShell, solutions created via GUI will not be accepted!

1. On the assigned virtual PC - Windows Server, log in to the Administrator account using the provided credentials.

2. *Create a new user account user1, which will be for a regular user, set the password to "Heslo123456". The user must be a member of the Users group. Document by listing commands that will show which users are set up on Windows and which groups they are members of.

3. Log in to the server with the new user1 account. Is login allowed? If not, why?

4. *Set the user1 account in the relevant user groups so that the given user can log in interactively to the server - in our case it is enough via the remote desktop.

       a. Document with a screenshot so that it is clear that user1 is logged in.

       b. Document by listing the commands that show which groups user1 is a member of Utility - it must not be an administrator, but a regular user who is allowed to log into the server the user

Task 2 - creating AD Domain

Evaluation: 0.5 b

Study material: https://dspace.uniba.sk/bitstream/handle/123456789/15/Ucebny_text_sprava_sieti_OS_linux_windows.pdf?sequence=3&isAllowed=y

Your task is to set up an Active Directory domain and "promote" your Windows server to a domain controller/ADDC domain controller.

- Rename your server - change its hostname to ADDC (good practice, after creating a domain, changing the hostname is more complicated)

- Set a static IP address for your server - view the current network parameters and set them statically - because it is not possible to set up a domain controller to have an IP address from DHCP (because the ADDC also includes a DNS server as part of the directory service)

- Install the Active Directory Domain Services role and DNS server. - Upgrade your server to a domain controller and create a new domain "yourname.local", while your first name must be substituted for your name. Solutions with a different domain name than your first name will not be accepted!

 - The server is restarted at the end. Sign up for it.

Task 3 - creating AD structure and regular user

Evaluation: 1 b

1.   Use the dedicated tools (GUI or PowerShell modules) to create an organizational structure for your domain. First, create organization units OUs for users, computers, and groups.
2.   Add a user to the business unit who will have a login name your first name, first name – your first name, last name – Smart. **Solutions with a name other than your first name will not be accepted!**
        Password set abc
3.   The system will tell you that such a password cannot be accepted. Find out what the password policy currently in force on your server is and, accordingly, create a custom password, which you will include in the solution, along with the wording of the corresponding password policy. **Warning - A different password policy is set on each of the Windows Servers**.
        The password policy can be detected in different ways, preferring in this case the procedure for detecting it using the GUI. Hint – you won't find a "password policy" tool using the GUI, there is no such thing in Windows, but these measures are specified within the "whole package" of measures.

Task 3b – Bonus

Rating: 1 b

Document your progress with screenshots and brief comments.

1.   Use Group Policy to set recommended password policy and account lock settings. The workaround must be implemented **by creating a custom Group Policy object so that the Group Policy object itself must be called "Password Poltika – YourFirstName"**. Solutions with a policy in the title that does not include your first name will not be accepted.

        Study material: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
        Set:
1.   password validity one year
2.   do not define the minimum age of the password - or set it so that it is not required
3.   password length 10 characters
4.   password complexity – enable + briefly explain in one sentence what characters the password must contain in order for it to be considered complex in the MS Windows environment
5.   to set your account to lock when you sign in to an unsuccessful sign-in, do the following:

Account Policies/ Account Lockout Policy

Policy	Setting
Account lockout duration	35 minutes
Account lockout threshold	7 invalid logon attempts
Reset account lockout counter after	35 minutes

6. Find out what command you need to use to apply the defined options in the policy, or justify whether you need to restart the server.

7. You can illustrate why it is important to set a Minimum password age with an example. Hint – take into account that in a corporate environment, a user's password is synchronized using the LDAP directory service and is used to sign in to Office365, AIS, internal information systems, VPNs, ...

8. Use printscreens to show where you can set group policy to force CTRL+ALT+DEL to press when signing in to your PC. At the same time, explain why it's a good idea to enable this setting.