Windows\_AD\_Search\_Accounts

10

Find the expired accounts that aren't disabled. List the last names in Alphabetical Order, separated with a comma, and no space between.

**get-aduser -filter 'enabled -eq $true' -Properties AccountExpirationDate | select Name, AccountExpirationDate**

Windows\_AD\_Search\_Emails

10

Find the unprofessional email addresses. List the email's domain.

**Get-ADUser -Filter {Name -like '\*'} -Properties \* | select EmailAddress | out-file -FilePath .\l**

**ist.txt**

**get-content -path .\list.txt | select-string '.com'**

scp -r .\list.txt garviel@10.11.0.6:~

get-aduser -filter {allowreversiblepasswordencryption -eq $TRUE -properies \*}

Windows\_AD\_Search\_Insider\_2

10

The flag is the name of the user who is requesting modified access rights.

Connect to the Warrior Share:

net use \* "\\file-server\warrior share"

**336-6754**

Windows\_AD\_Search\_Naming

10

Find the accounts that contain unprofessional information in the description.

List the last names in Alphabetical Order, separated by a comma, with no space.

Flag format: name,name

**Get-ADUser -Filter {Name -like '\*'} -Properties \* | select Description**

Windows\_AD\_Search\_Files

10

The flag is the unprofessionally-named file located somewhere on the Warrior Share.

Connect to the Warrior Share:

net use \* "\\file-server\warrior share"

**gci -recurse -filter "lulz.pdf"**

Windows\_AD\_Search\_Passwords

10

Find the following three accounts:

two accounts with passwords that never expire

get-aduser -filter \* -properties PasswordLastSet, PasswordExpired, PasswordNeverExpires | sort Name | ft Name, PasswordLastSet, PasswordExpired, PasswordNeverExpires

**Ibarra,Sanchez**

one account that has its password stored using reversible encryption

get-aduser -Filter 'userAccountControl -band 128' -Properties userAccountControl

**Brandywine,**

Windows\_Active\_Directory\_Basics\_7

10

What is the RID of the krbtgt account.

Example: S-1-5-21-1004336348-1177238915-682003330-[501]

- Get-ADUser -Identity 'krbtgt' -Properties Description

- RID is last 3 of SID

**502**