9

1 SAM

2 LSA

3 (Srv01) LSASS

4 PPL

5 mimikatz mimidrv.sys PPL

6 ( )

7 Web02 DPAPI

8 NTDS

9 Windows

10 API

11

12 Impacket LSA PTH Powershell

13 make_token runas

14 “ ”

15 **CreateProcessAsUserCreateProcessWithTokenCreateProcessWithLogon**, **LogonUser** API

16

17

18 PTH

19 Mimikatz PTH LSASS Impacket

20 Impacket keytab Web01 keytab keytab ( )

Revision #8
Created 10 September 2022 16:41:40 by
Updated 28 December 2023 01:31:56 by