Development of techniques to remove Kerberos credentials from Windows Systems.

Nick Offerman
Steffan Roobol

04-07-2019

Introduction

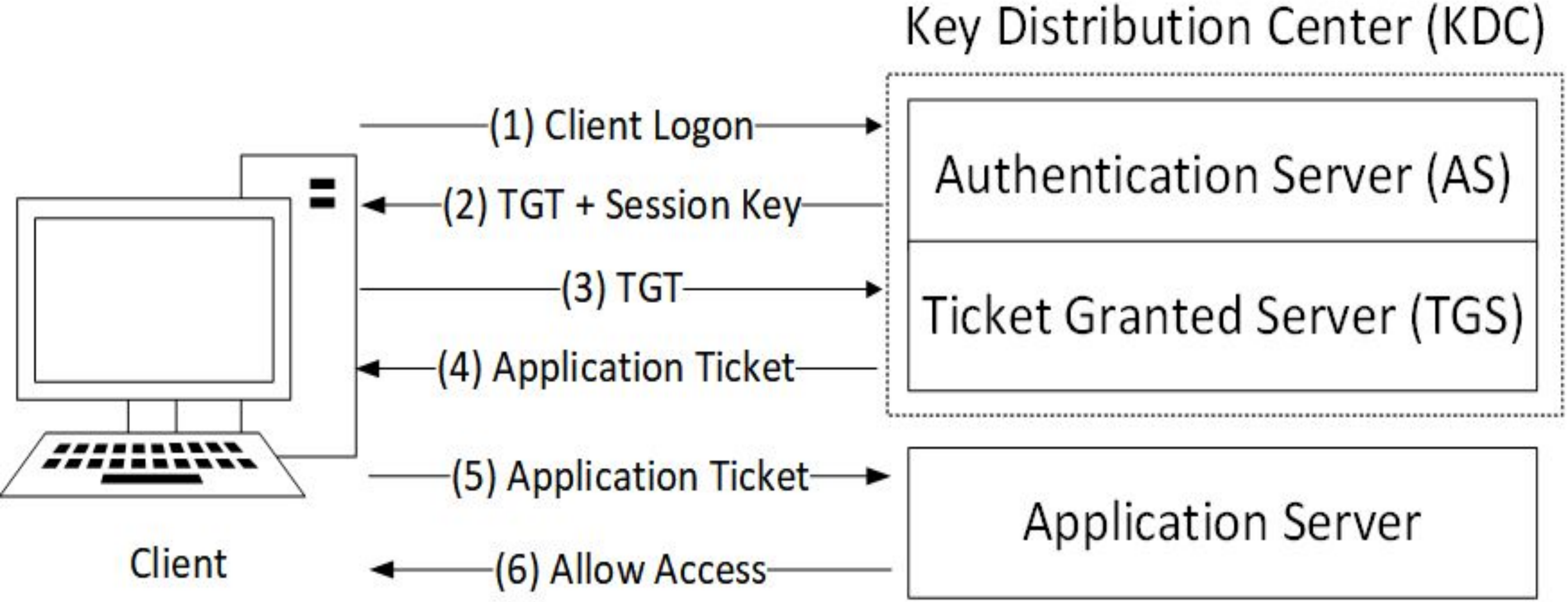


Figure 1: Kerberos Protocol

Problem

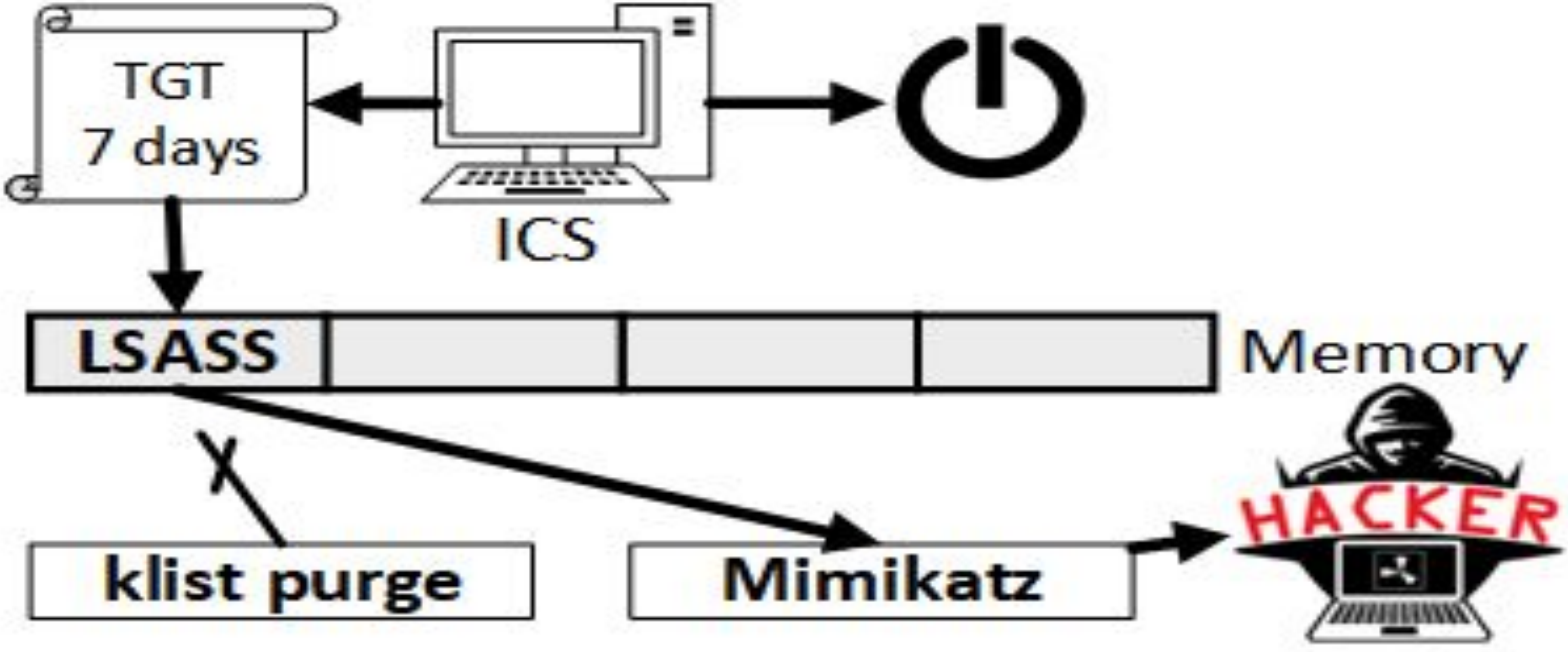


Figure 1: the LSASS process and Mimikatz.

Research Questions

How can Kerberos credentials be completely purged out of a Windows Operating System without rebooting the system?

(1) Mimikatz

(2) klist

(3) Remove credentials

Related Work

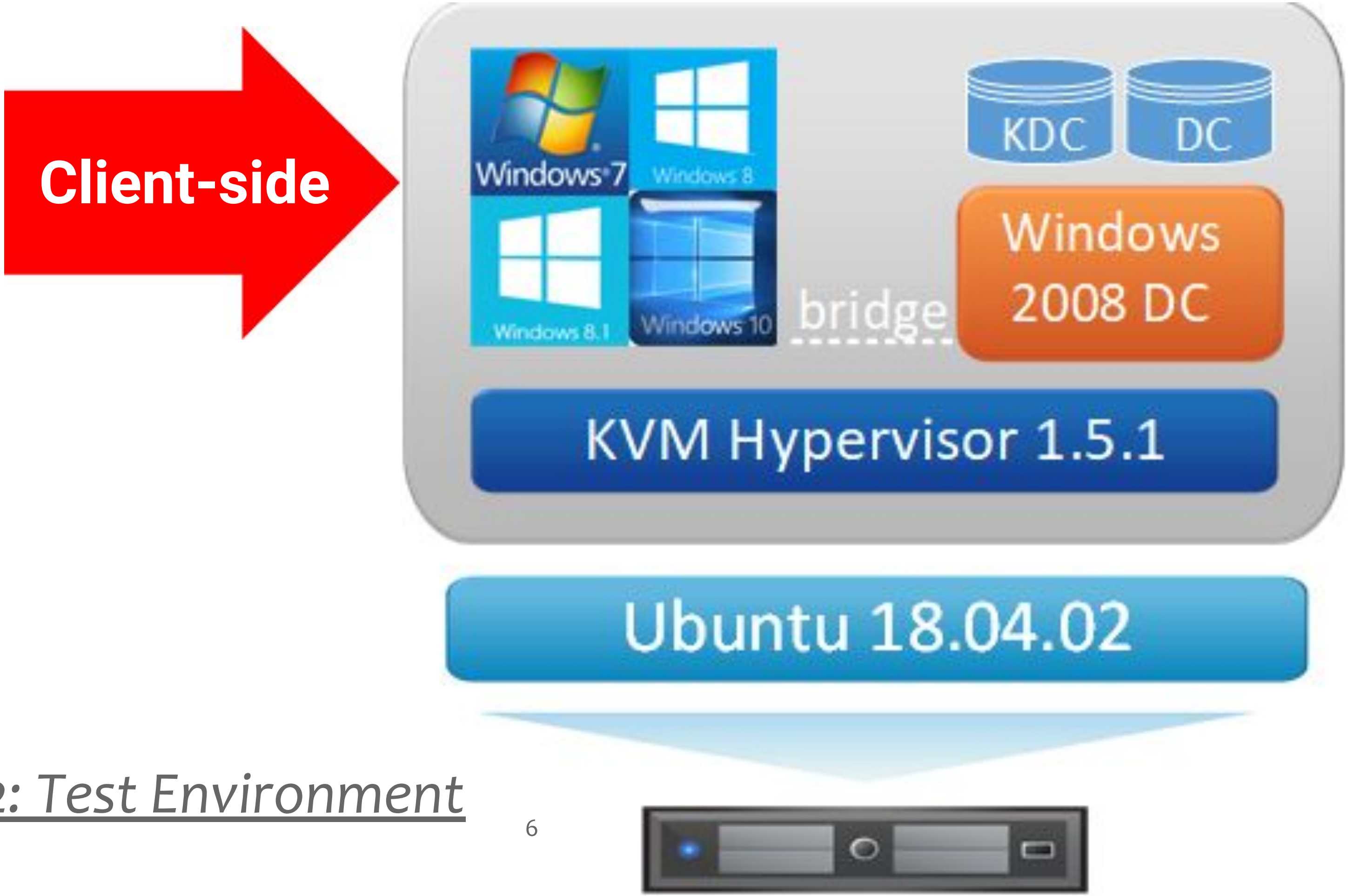
Benjamin Delpy created open-source Mimikatz tool

- *Read out credentials from LSASS*
- *Forge Kerberos tickets*

Blog posts

- *Anti-Mimikatz (debug privilege)*
- *Registry keys*
- *Group policies*

Methods - Test environment



Client-side

Windows 7

Windows 8

Windows 8.1

Windows 10

bridge

KDC

DC

Windows 2008 DC

KVM Hypervisor 1.5.1

Ubuntu 18.04.02

Figure 2: Test Environment

Methods - Experiments

- Analyse Mimikatz
- Analyse klist
- Create tool
- Test reading out of credentials

Methods - Experiments

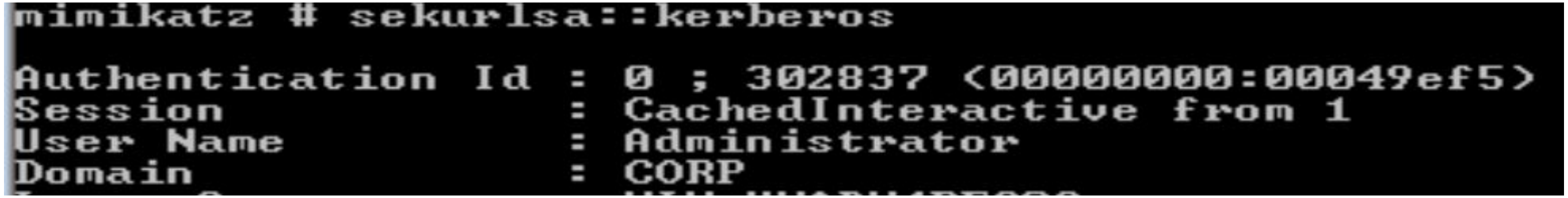
	Experiment	7	8	8.1	10
Baseline	*klist*	Yes	Yes	Yes	Yes
	kerberos::list	Yes	No	No	No
	sekurlsa::kerberos	Yes	Yes	No	No
After klist purge	*klist*	?	?	?	?
	kerberos::list	?	?	?	?
	sekurlsa::kerberos	?	?	?	?
After tool	*klist*	?	?	?	?
	kerberos::list	?	?	?	?
	sekurlsa::kerberos	?	?	?	?

Table 1: Retrieving credentials on Windows systems before and after commands.

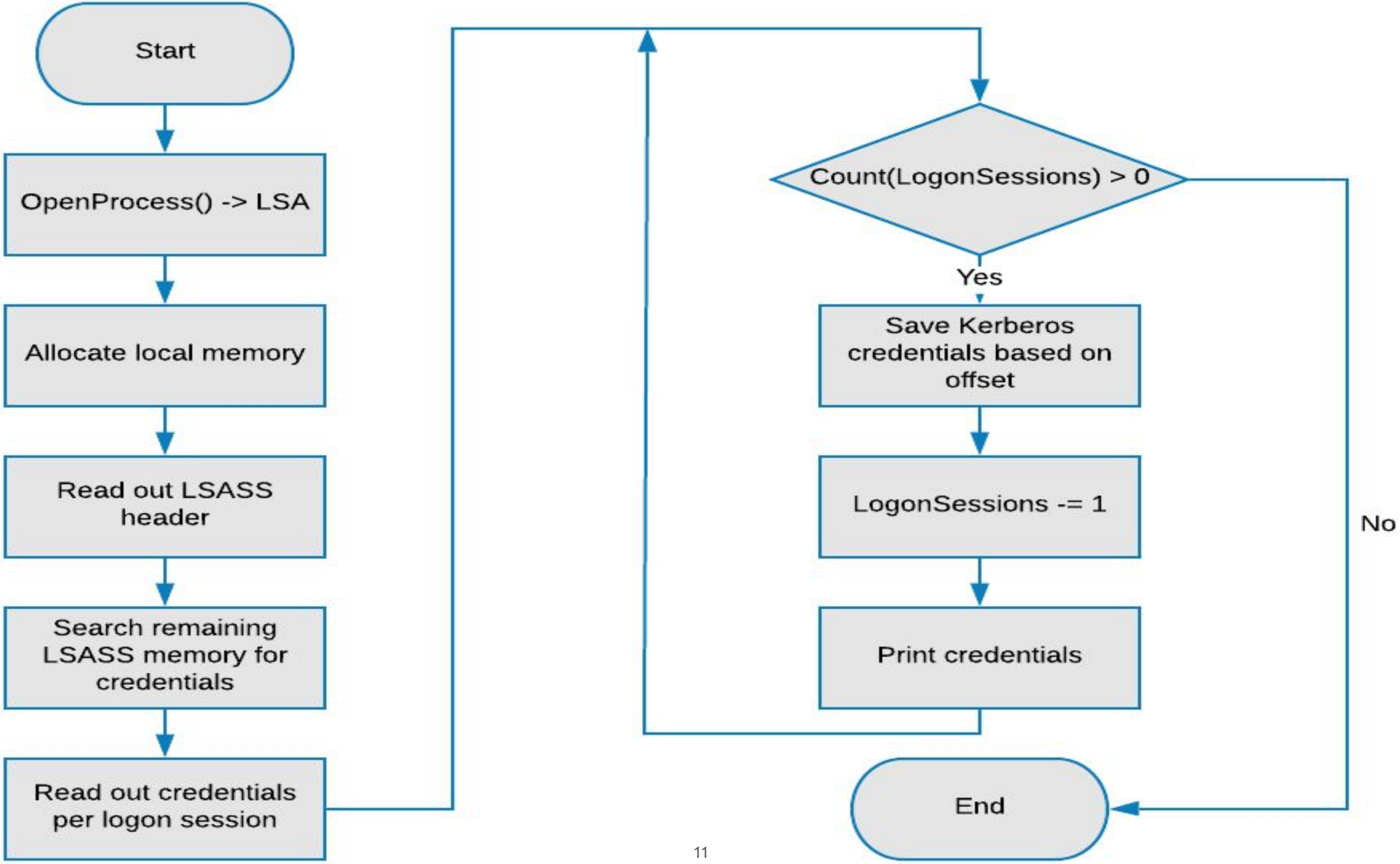
Methods - Tools

- Analysis Mimikatz code
  - Visual Studio 2017
- Analysis klist executable
  - IDA
  - x64dbg
- Programming
  - C
  - Windows Powershell

Results - Mimikatz analysis

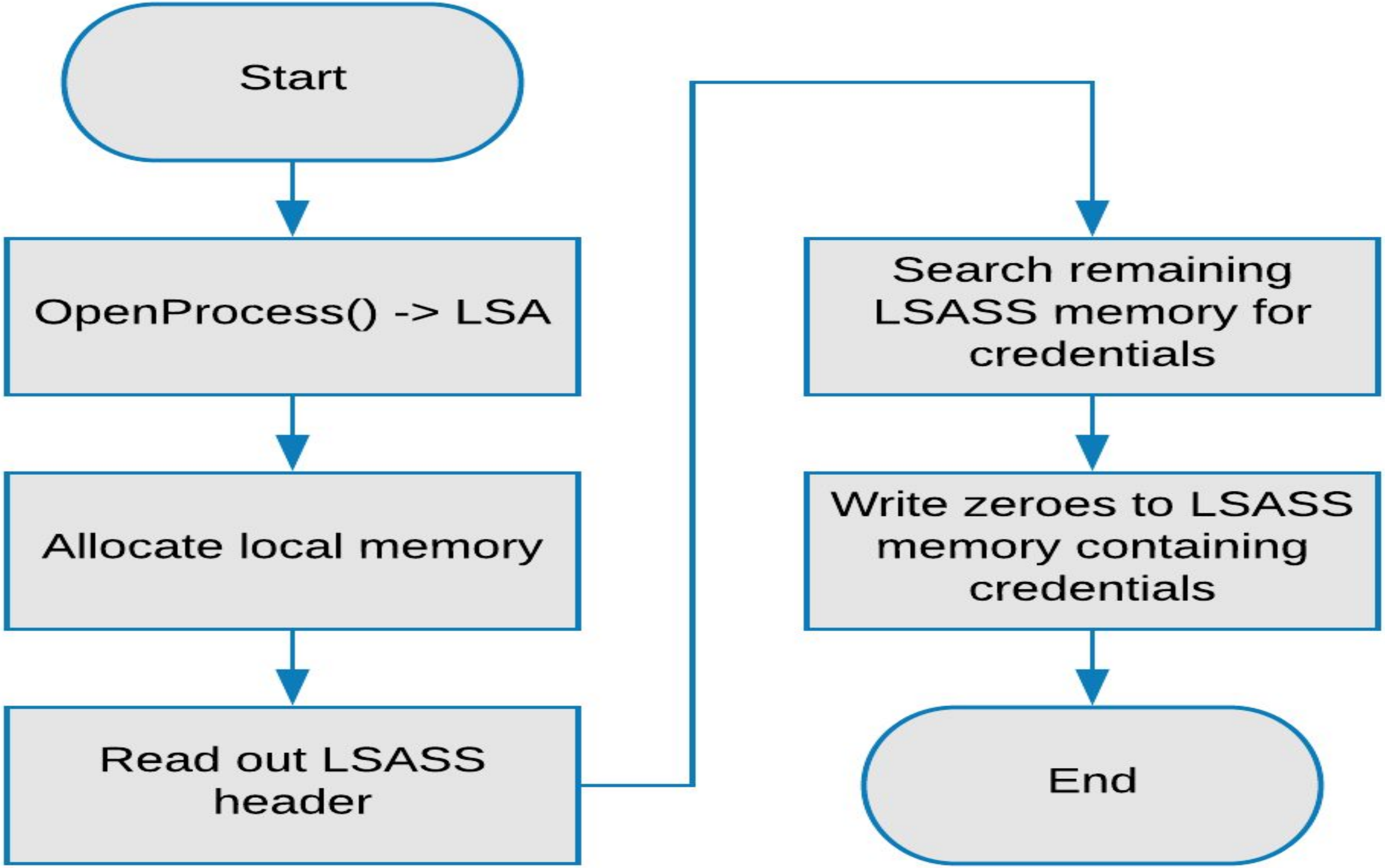


```
mimikatz # sekurlsa::kerberos

Authentication Id : 0 ; 302837 (00000000:00049ef5)
Session           : CachedInteractive from 1
User Name         : Administrator
Domain            : CORP
```


Start
OpenProcess() -> LSA
Allocate local memory
Read out LSASS header
Search remaining LSASS memory for credentials
Read out credentials per logon session
Count(LogonSessions) > 0
Yes
Save Kerberos credentials based on offset
LogonSessions -= 1
Print credentials
No
End

Results - Overwriting LSASS

- Mimikatz can read? We can write.
- Right after searching the credential blob



Start

OpenProcess() -> LSA

Allocate local memory

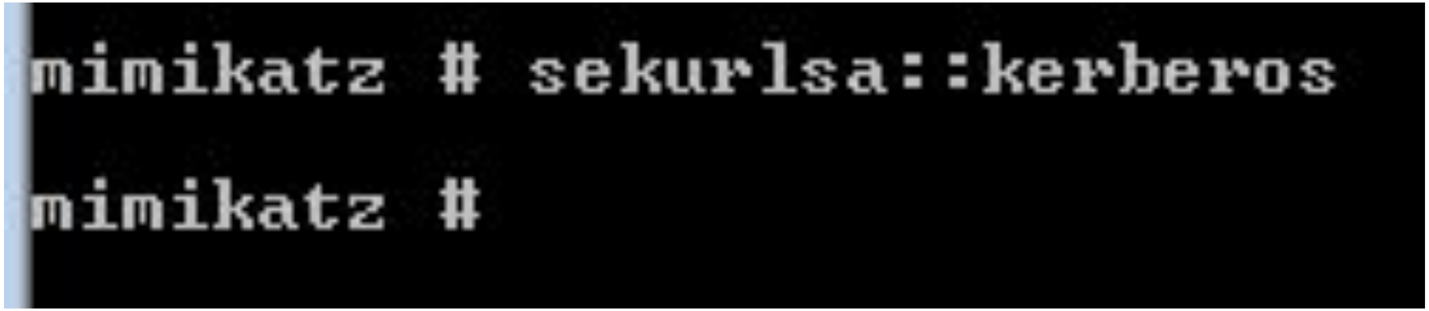
Read out LSASS header

Search remaining LSASS memory for credentials

Write zeroes to LSASS memory containing credentials

End

Results - Overwriting LSASS



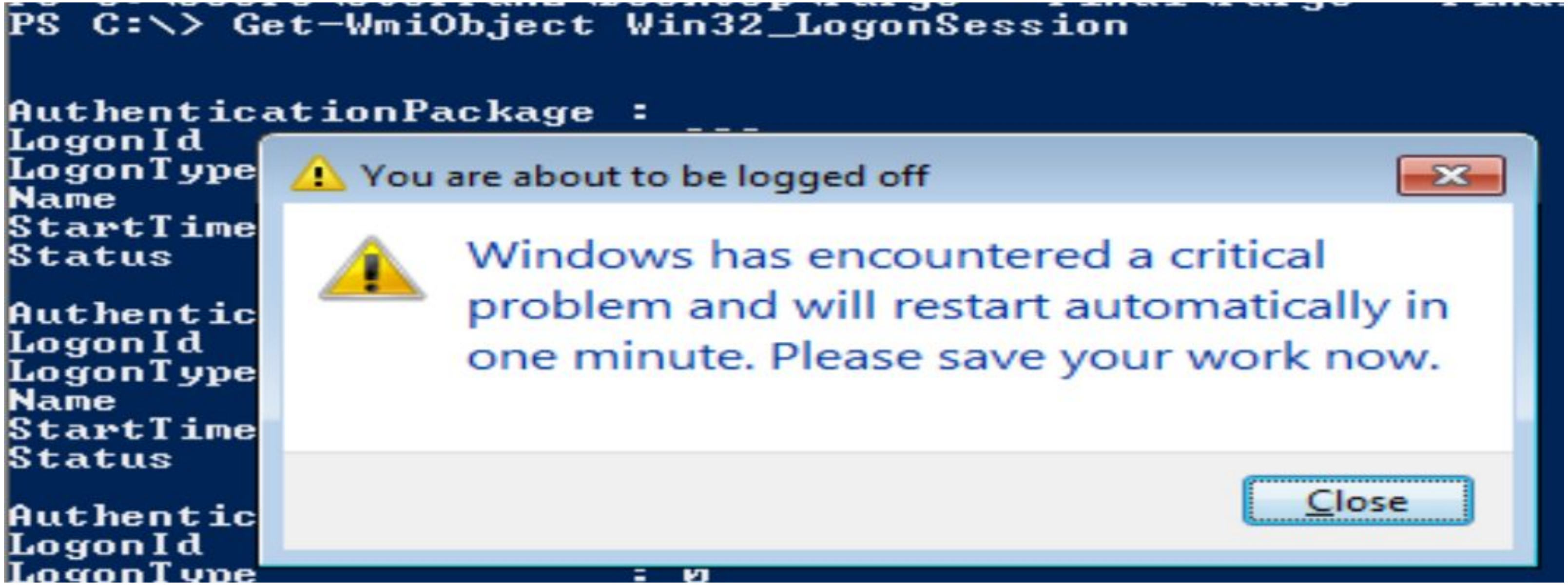
```
mimikatz # sekurlsa::kerberos

mimikatz #
```

Results - Overwriting LSASS

	Experiment	**7**	**8**	**8.1**	**10**
Baseline	*klist*	Yes	Yes	Yes	Yes
	kerberos::list	Yes	No	No	No
	sekurlsa::kerberos	Yes	Yes	No	No
After overwriting	*klist*	Yes	Yes	Yes	Yes
	kerberos::list	Yes	No	No	No
	sekurlsa::kerberos	No	No*	No*	No*

Table 2: Retrieving credentials on Windows systems before and after overwriting.

Results - Overwriting LSASS

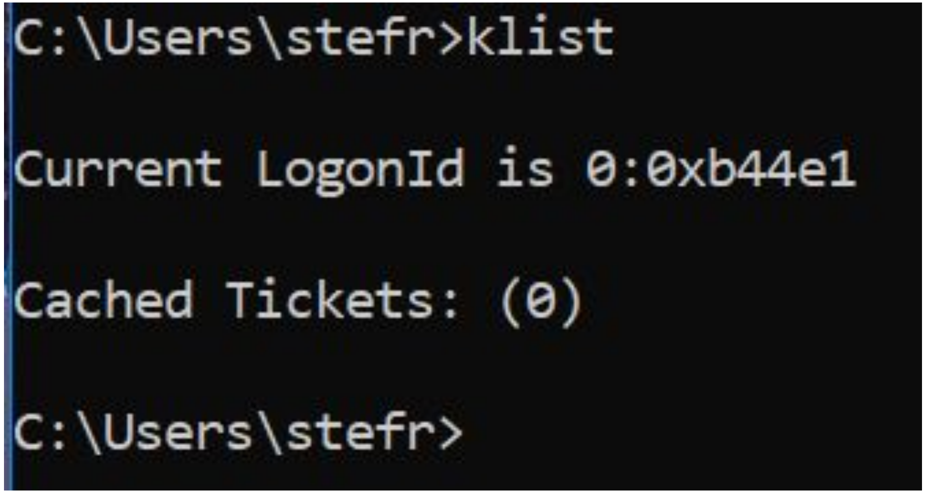


```
PS C:\> Get-WmiObject Win32_LogonSession

AuthenticationPackage :
LogonId
LogonType
Name
StartTime
Status

Authentic
LogonId
LogonType
Name
StartTime
Status

Authentic
LogonId
LogonType                 : 0
```

You are about to be logged off

Windows has encountered a critical problem and will restart automatically in one minute. Please save your work now.

Results - klist command



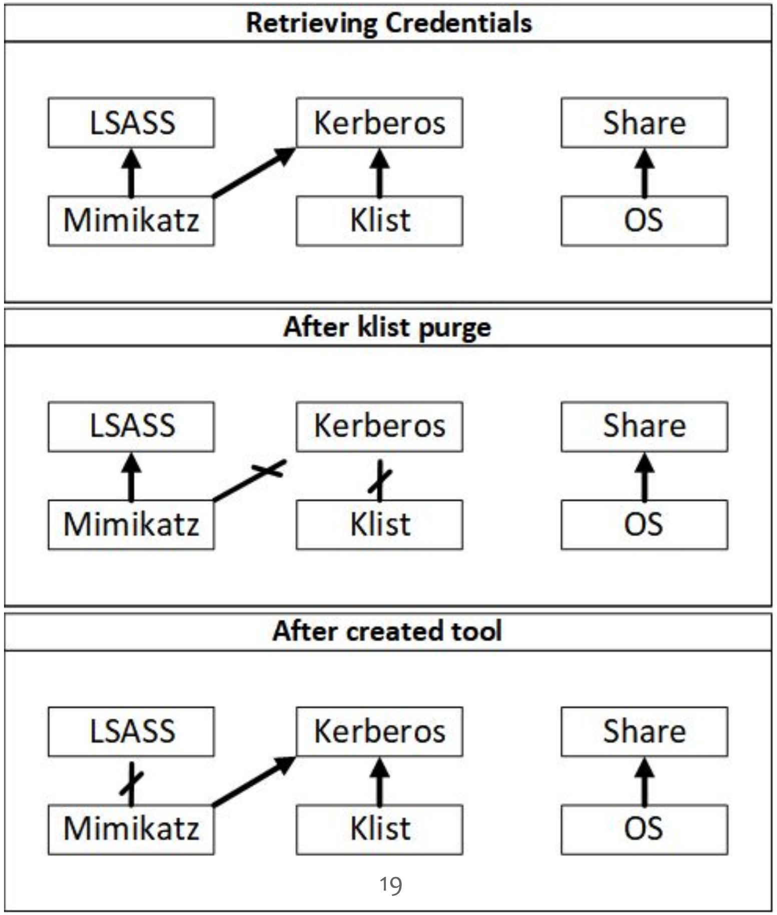
```
C:\Users\stefr>klist

Current LogonId is 0:0xb44e1

Cached Tickets: (0)

C:\Users\stefr>
```

Results - klist command

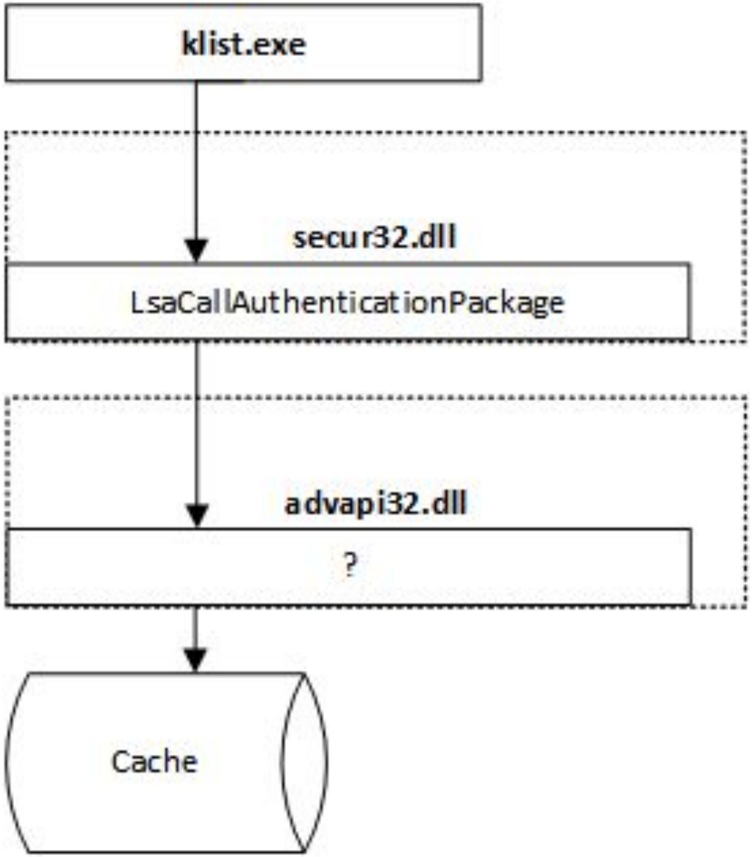
	Experiment	7	8	8.1	10
Baseline	*klist*	Yes	Yes	Yes	Yes
	kerberos::list	Yes	No	No	No
	sekurlsa::kerberos	Yes	Yes	No	No
After klist purge	*klist*	No	No	No	No
	kerberos::list	No	No	No	No
	sekurlsa::kerberos	Yes	Yes	No	No

Table 3: Retrieving credentials on Windows systems before and after klist purge.

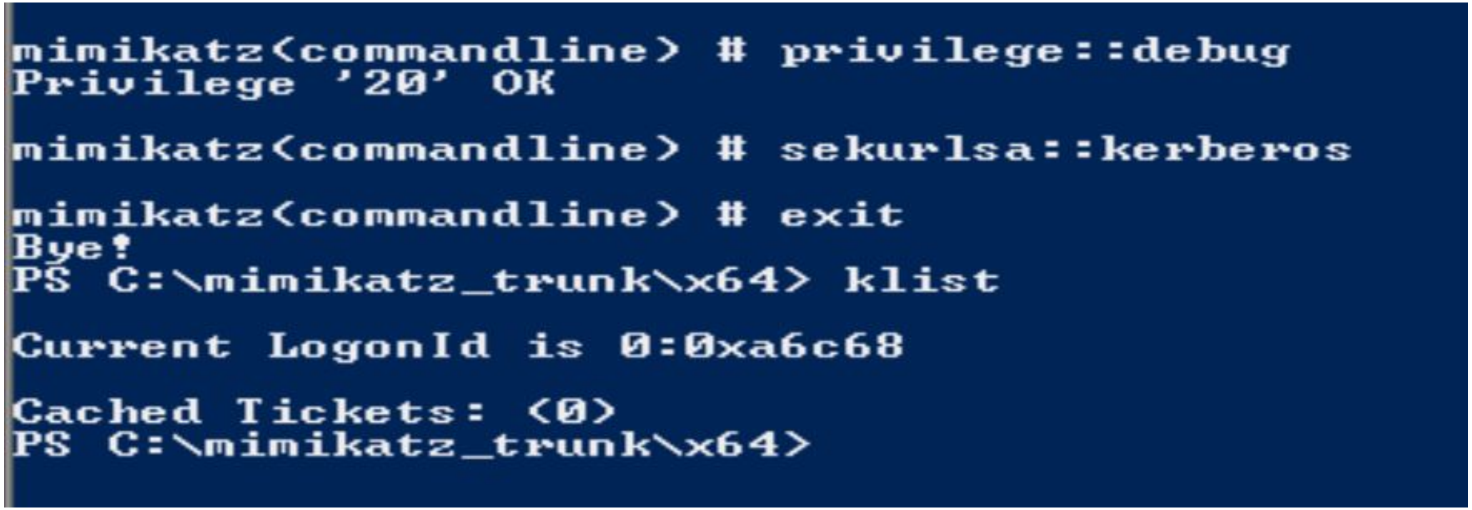
Results - klist command



Results - klist command



Results - PowerShell script



```
mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::kerberos

mimikatz(commandline) # exit
Bye!
PS C:\mimikatz_trunk\x64> klist

Current LogonId is 0:0xa6c68

Cached Tickets: (0)
PS C:\mimikatz_trunk\x64>
```

Discussion

- Mimikatz:
  - LSASS memory
  - Windows API calls
- klist:
  - Kerberos memory
- Purge tool:
  - Clears both locations

Discussion

- But…
  - Get-WmiObject Win32_LogonSession
  - Limitations:
    - Tool overwrites all credentials
    - Windows 7
    - Kerberos memory

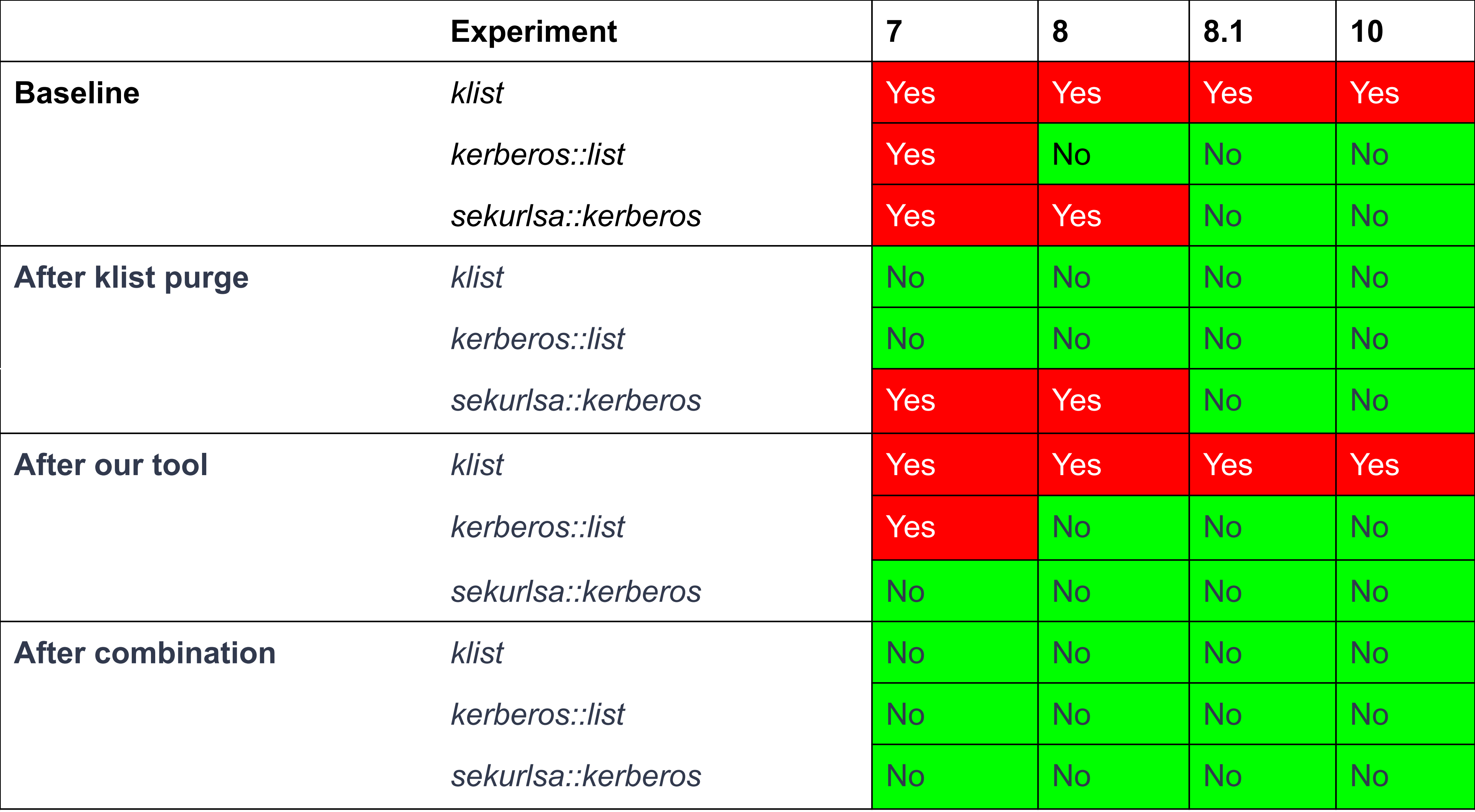
Future Work

- Specific credential removal
- Expand for other OSs
- Further explore klist

Conclusion

How can Kerberos credentials be completely purged out of a Windows Operating System without rebooting the system?

	Read	**Remove**
LSASS Memory	Mimikatz	Tool
Kerberos Memory	Klist	Klist purge



	Experiment	7	8	8.1	10
Baseline	*klist*	Yes	Yes	Yes	Yes
	kerberos::list	Yes	No	No	No
	sekurlsa::kerberos	Yes	Yes	No	No
After klist purge	*klist*	No	No	No	No
	kerberos::list	No	No	No	No
	sekurlsa::kerberos	Yes	Yes	No	No
After our tool	*klist*	Yes	Yes	Yes	Yes
	kerberos::list	Yes	No	No	No
	sekurlsa::kerberos	No	No	No	No
After combination	*klist*	No	No	No	No
	kerberos::list	No	No	No	No
	sekurlsa::kerberos	No	No	No	No

Table 4: Retrieving credentials on Windows systems before and after commands.

Thank You!

Questions?