

Abdllrahman Alghanim

LAB 10 - Malware Analysis

CIS4204

```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# file /usr/share/windows-resources/mimikatz/x64/mimikatz.exe
/usr/share/windows-resources/mimikatz/x64/mimikatz.exe: PE32+ executable (console) x86-64, for MS Windows, 6 sections

(root@kali)-[~]
# md5sum /usr/share/windows-resources/mimikatz/x64/mimikatz.exe
29efd64dd3c7fe1e2b022b7ad73a1ba5 /usr/share/windows-resources/mimikatz/x64/mimikatz.exe

(root@kali)-[~]
#
```

```
root@kali: ~
File Actions Edit View Help
Kali NetHunter - Exploit-DB - Google Hacking DB

File: /usr/share/windows-res ASCII Offset: 0x00000000 / 0x0014ADFF (%00)
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 Z.....
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000030 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 .....
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 .....!..L.!Th
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F s program canno
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 be run in DOS
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 ode....$.
00000080 20 70 D7 1D 64 11 B9 4E 64 11 B9 4E 64 11 B9 4E p..d..Nd..Nd..N
00000090 6D 69 2C 4E 65 11 B9 4E 6D 69 3A 4E 5A 11 B9 4E i,Ne..Nmi:NZ..N
000000A0 6D 69 3D 4E 74 11 B9 4E 6D 69 2A 4E 66 11 B9 4E i=Nt..Nmi*Nf..N
000000B0 02 FF 72 4E 62 11 B9 4E FF FA 72 4E 66 11 B9 4E .rNb..N..rNf..N
000000C0 12 8C D4 4E 67 11 B9 4E 7A 43 3D 4E 66 11 B9 4E ..Ng..NzC=Nf..N
000000D0 12 8C C2 4E 57 11 B9 4E 64 11 B8 4E FA 13 B9 4E ..NW..Nd..N...N
000000E0 43 D7 C7 4E 65 11 B9 4E 6D 69 30 4E 16 11 B9 4E ..Ne..Nmi0N...N
000000F0 6D 69 2D 4E 65 11 B9 4E 6D 69 28 4E 65 11 B9 4E i-Ne..Nmi(Ne..N
00000100 52 69 63 68 64 11 B9 4E 00 00 00 00 00 00 00 00 ichd..N.....
00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000120 50 45 00 00 64 86 06 00 67 8E 28 63 00 00 00 00 E..d...g.(c...
00000130 00 00 00 00 F0 00 22 00 0B 02 09 00 00 F8 0C 00 .....
00000140 00 C2 07 00 00 00 00 00 E8 98 0C 00 00 10 00 00 ..@.....
00000150 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 ..@.....
00000160 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 .....
00000170 00 F0 14 00 00 04 00 00 00 00 00 00 03 00 40 81 .....@.
00000180 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 .....
^G Help ^C Exit (No Save) ^T goTo Offset ^X Exit and Save ^W Search
```

```
kali@kali: ~  
File Actions Edit View Help  
CaL Ba  
'V}L&U|  
,PoL,Po  
!A\+!B]  
W[]C6  
dvvg7  
Zkj_9  
;^I*Ro  
_  
*#9M  
4Kb%  
;L`bFVe  
;Um07Tn  
@VhR<Ui  
.Jbv+Jd  
Owqm4  
rxw2I  
(1>?  
/G^E`  
8Pido  
!Diy  
+NkV  
-n: command not found  
  
(kali@kali)-[~]  
$
```

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
  
(kali@kali)-[~]  
$ strings /usr/share/windows-resources/mimikatz/x64/mimikatz.exe  
_n 15 | more  
!This program cannot be run in DOS mode.  
Nmi,Ne  
Nmi:NZ  
Nmi=Nt  
Nmi*Nf  
NzC=Nf  
Nmi0N  
Nmi-Ne  
Nmi(Ne  
NRichd  
.text  
`.rdata  
@.data  
.pdata  
@.rsrc  
@.reloc  
WATAUH  
L$BD  
l$@D  
d$AD  
d$CfA;
```