

Compte-rendu Ydays JOUR 1 - 21/10/2020

*pc fixe

1. Préparation des VM pour la réalisation de Pentesting

- ⇒ Transfert de ma VM Kali Linux de mon pc portable à mon pc fixe
- ⇒ Et installation/préparation de la VM Metasploit 2 sur VMware Workstation*

2. Réalisation / Exercices sur le site Root-me

- ⇒ Challenge Root-me : Cracking PE x86 – 0 protection

<https://www.root-me.org/fr/Challenges/Cracking/PE-x86-0-protection>

- ⇒ Présentation de ce que j'ai obtenu aujourd'hui après maintes recherches :
 - Tout d'abord j'ai téléchargé le challenge : ch15.exe
 - La 1^{ère} commande que j'ai fait « rabin2 -I ... » (je ne sais pas précisément ce que ça fait, mais je vois que ça me donne les caractéristiques de mon fichier .exe, sont architecture x86 ou encore la classe PE36.


```
pierre@kali:~/Downloads$ ls
ch15.exe  ch2.dmp  ch2.tbz2  ch5.zip  journal.jpg
pierre@kali:~/Downloads$ rabin2 -I ch15.exe
arch      x86
baddr     0x400000
binsz     11776
bintype   pe
bits      32
canary    false
retguard  false
class     PE32
cmp.csum  0x0000af8c
compiled  Thu Oct 18 02:17:55 2012
crypto    false
endian    little
havecode  true
hdr.csum  0x0000af8c
laddr     0x0
lang      c
linenum   true
lsyms     true
machine   i386
maxopisz  16
minopisz  1
nx        false
os        windows
overlay   false
pcalign   0
pic       false
relocs    true
signed    false
sanitiz   false
static    false
stripped  true
subsys    Windows CUI
va        true

[0x004014e0]> ie
[Entrypoints]
vaddr=0x004014e0 paddr=0x000008e0 haddr=0x000000a8 type=program
1 entrypoints

[0x004014e0]> iz
[Strings]
Num Paddr Vaddr Len Size Section Type String
000 0x00002000 0x00404000 30 31 (.rdata) ascii _set_invalid_parameter_handler
001 0x00002020 0x00404020 12 13 (.rdata) ascii libgcj_s.dll
002 0x0000202d 0x0040402d 19 20 (.rdata) ascii _Jv_RegisterClasses
003 0x00002044 0x00404044 14 15 (.rdata) ascii Usage: %s pass
004 0x00002053 0x00404053 12 13 (.rdata) ascii Gratz man :)
005 0x00002060 0x00404060 14 15 (.rdata) ascii Wrong password
006 0x00002074 0x00404074 13 14 (.rdata) ascii Unknown error
007 0x00002084 0x00404084 42 43 (.rdata) ascii _matherr(): %s in %s(%g, %g) (retval=%g)\n
008 0x000020b0 0x004040b0 30 31 (.rdata) ascii Argument domain error (DOMAIN)
009 0x000020cf 0x004040cf 27 28 (.rdata) ascii Argument singularity (SIGN)
010 0x000020ec 0x004040ec 31 32 (.rdata) ascii Overflow range error (OVERFLOW)
011 0x0000210c 0x0040410c 53 54 (.rdata) ascii The result is too small to be represented (UNDERFLOW)
012 0x00002144 0x00404144 34 35 (.rdata) ascii Total loss of significance (TLOSS)
013 0x00002168 0x00404168 36 37 (.rdata) ascii Partial loss of significance (PLOSS)
014 0x000021a8 0x004041a8 27 28 (.rdata) ascii Mingw-w64 runtime failure:\n
015 0x000021c4 0x004041c4 31 32 (.rdata) ascii Address %p has no image-section
016 0x000021e4 0x004041e4 48 49 (.rdata) ascii VirtualQuery failed for %d bytes at address %p
017 0x00002218 0x00404218 49 50 (.rdata) ascii Unknown pseudo relocation protocol version %d.\n
018 0x0000224c 0x0040424c 41 42 (.rdata) ascii Unknown pseudo relocation bit size %d.\n
019 0x00002278 0x00404278 10 22 (.rdata) utf16le msvcrt.dll
```

Ensuite j'ai lancé radare2 (r2) avec le fichier : « r2 ch15.exe » et ensuite, je pouvais utiliser des commandes.

- Après je me suis renseigné un peu plus et j'ai trouvé Ollydbg, c'est un logiciel, plutôt un debugger x86 qui permet l'analyse du code binaire (lien : <http://www.ollydbg.de/>).




OllyDbg

Progress in [OllyDbg 64](#) (05-Feb-201
[VERSION 2.01](#) (27-Sep-2013)
+ Disassembler v2.01, preliminary version

Off-topic 1: [PaperBack](#) - backups on the paper (v
Off-topic 2: [Jasan](#) - graphical interface to the Hercu

index
[Main page](#)
[What's new](#)
[Requirements](#)
[Privacy](#)
[Download](#)
[Quick start](#)
[PDK](#)
[Schemes](#)
[FAQs](#)
[Sources](#)

Files
[Odbg200.zip](#)
[Odbg110.zip](#)
[Odbg108b.zip](#)
[Plug110.zip](#)
[Disasm.zip](#)
[Cmdline.zip](#)



OllyDbg is a 32-bit assembler level analysing debugger for Microsoft® Windows®. Emphasis on **binary c**

- J'ai donc téléchargé Ollydbg : Odbg200.zip que j'ai ensuite unzip pour pouvoir exécuter le programme correctement : « unzip odbg200.zip ».

```
pierre@kali:~$ cd Downloads/
pierre@kali:~/Downloads$ ls
odbg200.zip
pierre@kali:~/Downloads$ unzip odbg200.zip
Archive:  odbg200.zip
  inflating: help.pdf
  inflating: ollydbg.exe
pierre@kali:~/Downloads$ ls
help.pdf  odbg200.zip  ollydbg.exe
pierre@kali:~/Downloads$
```

- Il se trouve que je voulais lancer le programme avec la commande « wine ollydbg.exe », mais wine n'était pas connu, il m'a donc fallu l'installer, mais pour installer « wine » cela n'a pas marché directement (cf. les 2 prochaines captures).

```
pierre@kali:~$ sudo dpkg --add-architecture i386
[sudo] password for pierre:
pierre@kali:~$ sudo apt-get update
Ign:1 http://security.kali.org/kali-security sana/updates InRelease
Err:2 http://security.kali.org/kali-security sana/updates Release
      404 Not Found [IP: 192.99.200.113 80]
Get:3 http://ftp.free.fr/pub/kali kali-rolling InRelease [30.5 kB]
Ign:4 http://http.kali.org/kali sana InRelease
Hit:5 http://old.kali.org/kali moto InRelease
Get:6 http://ftp.free.fr/pub/kali kali-rolling/main amd64 Packages [16.7 MB]
Err:7 http://http.kali.org/kali sana Release
      404 Not Found [IP: 192.99.200.113 80]
Get:8 http://old.kali.org/kali moto/main i386 Packages [10.9 MB]
Get:9 http://ftp.free.fr/pub/kali kali-rolling/main i386 Packages [16.6 MB]
Get:10 http://ftp.free.fr/pub/kali kali-rolling/contrib i386 Packages [92.3 kB]
Get:11 http://ftp.free.fr/pub/kali kali-rolling/contrib amd64 Packages [100 kB]
Get:12 http://ftp.free.fr/pub/kali kali-rolling/non-free i386 Packages [169 kB]
Get:13 http://ftp.free.fr/pub/kali kali-rolling/non-free amd64 Packages [200 kB]
Get:14 http://old.kali.org/kali moto/non-free i386 Packages [163 kB]
Get:15 http://old.kali.org/kali moto/contrib i386 Packages [79.4 kB]
Reading package lists ... Done
E: The repository 'http://security.kali.org/kali-security sana/updates Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
E: The repository 'http://http.kali.org/kali sana Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
```

```

pierre@kali:~$ sudo apt-get install wine
Reading package lists... Done
Building dependency tree
Reading state information... Done
Some packages could not be installed. This may mean that you have
requested an impossible situation or if you are using the unstable
distribution that some required packages have not yet been created
or been moved out of Incoming.
The following information may help to resolve the situation:

The following packages have unmet dependencies:
 libc6-dev : Breaks: libgcc-9-dev (< 9.3.0-5~) but 9.2.1-22 is to be installed
E: Error, pkgProblemResolver::Resolve generated breaks, this may be caused by held packages.
pierre@kali:~$

```

- Je me suis donc renseigné un peu plus et plusieurs personnes rencontrent ce problème et la solution était d'aller dans le fichier source d'apt avec la commande : « `sudo nano /etc/apt/sources.list` ». A l'intérieur de ce fichier, il manquait 2 lignes (cf. capture ci-dessous).

```

deb http://http.kali.org/kali kali-rolling main non-free contrib
deb-src http://http.kali.org/kali kali-rolling main non-free contrib

```

- Après ré-écriture du fichier, j'ai dû installer « gdebi » car pour installer « wine » il manquait quelques composants nécessaires ;

```

pierre@kali:~$ sudo apt-get install gdebi
Reading package lists... Done
Building dependency tree
Reading state information... Done

```

```

pierre@kali:~$ sudo apt install wine
Reading package lists... Done
Building dependency tree
Reading state information... Done

```

- J'ai fait l'installation de « wine » et pour voir si cela a bien été effectué, on peut vérifier la version de celle-ci : « `wine --version` ».
- Après vérification, j'ai pu enfin lancer Ollydbg avec la commande « `wine ollydbg.exe` ».

```

pierre@kali:~$ wine --version
wine-5.0 (Debian 5.0-4)
pierre@kali:~$ cd Downloads/
pierre@kali:~/Downloads$ wine ollydbg.exe

```

- Par miracle, le programme s'est lancé correctement et j'ai pu ouvrir avec celui-ci le fichier du challenge que j'ai téléchargé au début.

File View Debug Trace Options Windows Help

CPU - main thread, module ch15

Address	Disassembly	Comment
00401474	85DB TEST EBX,EBX	
00401476	C705 E0534000 MOV DWORD PTR DS:[4053E0],2	
00401480	0F85 FAFDFFFF JNE 00401280	
00401486	C74424 04 00 MOV DWORD PTR SS:[ESP+4],0	Arg2 ==> 0
0040148E	C70424 DC5341 MOV DWORD PTR SS:[ESP],OFFSET 004053DC	Arg1 ==> ch15.4053DC
00401495	E8 76130000 CALL 00402810	ch15.00402810
0040149A	83EC 08 SUB ESP,8	
0040149D	E9 DEFDFDFFFF JMP 00401280	
004014A2	891424 MOV DWORD PTR SS:[ESP],EDX	
004014A5	FF15 30614000 CALL DWORD PTR DS:[<&KERNEL32.GetStartupInfoA@77D408B5>]	
004014AB	83EC 04 SUB ESP,4	
004014AE	66:90 NOP	Superfluous operand size prefix
004014B0	E9 44FDFDFFFF JMP 004011F9	
004014B5	C705 E0534000 MOV DWORD PTR DS:[4053E0],1	
004014BF	C74424 04 18 MOV DWORD PTR SS:[ESP+4],OFFSET 00407010	
004014C7	C70424 0C7041 MOV DWORD PTR SS:[ESP],OFFSET 0040700C	
004014CE	E8 C5130000 CALL <JMP.&msvcrt._initterm>	
004014D3	E9 92FDFDFFFF JMP 0040126A	
004014D8	890424 MOV DWORD PTR SS:[ESP],EAX	
004014DB	E8 C0130000 CALL <JMP.&msvcrt.exit>	
004014E0	83EC 0C SUB ESP,0C	
004014E3	C705 40504000 MOV DWORD PTR DS:[405040],0	
004014ED	E8 DE0E0000 CALL 004023D0	
004014F2	83C4 0C ADD ESP,0C	
004014F5	E9 96FCFFFF JMP 00401190	
004014FA	8DB6 00000000 LEA ESI,[ESI]	
00401500	83EC 0C SUB ESP,0C	
00401503	C705 40504000 MOV DWORD PTR DS:[405040],1	
0040150D	E8 BE0E0000 CALL 004023D0	
00401512	83C4 0C ADD ESP,0C	
00401515	E9 76FCFFFF JMP 00401190	
0040151A	8DB6 00000000 LEA ESI,[ESI]	
00401520	56 PUSH ESI	
00401521	53 PUSH EBX	
00401522	83EC 14 SUB ESP,14	
00401525	8B5C24 20 MOV EBX,DWORD PTR SS:[ARG.1]	
00401529	8B03 MOV EAX,DWORD PTR DS:[EBX]	
0040152B	8B00 MOV EAX,DWORD PTR DS:[EAX]	
0040152D	3D 910000C0 CMP EAX,C0000091	
00401532	77 43 JA SHORT 00401577	
00401534	3D 8D0000C0 CMP EAX,C000008D	

Imm=0000000C (decimal 12.)
ESP=0060FF34

Address	Hex dump	ASCII
00403000	FF FF FF FF FF 00 00 00 FF FF FF FF FF FF FF FF	yyyyy...yyyyyyy
00403010	40 29 40 00 02 00 00 00 4E E6 40 8B B1 19 BF 44	@)@. . . .Na@»± LD
00403020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Address	Hex dump	ASCII
0060FF30	003FF000	.07.
0060FF3C	7B454CFC	ULE{
0060FF40	7B454CFC	ULE{
0060FF44	7B454CFC	ULE{

0060FF34 7B454882 .HE{ RETURN to kernel3
 0060FF38 003FF000 .07.
 0060FF3C 7B454CFC ULE{ RETURN from kerne:
 0060FF40 7B454CFC ULE{ RETURN from kerne:
 0060FF44 7B454CFC ULE{ RETURN from kerne:

Lien pour la prochaine fois : <https://resources.infosecinstitute.com/reverse-engineering-ollydbg/>

Après tout ceci, j'ai arrêté pour l'instant. Je continuerai le rapport plus tard (21/10/20).