RADARE2 WORKSHOP

Writing a crack for
October 22, 2015

hack.lu 2015
Julien (jvoisin) Voisin

- French
- Freshly graduated
- I don’t know Windows
Piracy is **bad**, m’kay.
WHAT IS THIS?
AND WHAT IS THIS?
Time to write a compatibility enhancement hotfix!
Time to write a compatibility enhancement hotfix!

While knowing close to nothing about the Windows world.
In your virtual machine, in the nocd folder.
FINDING THE RIGHT FUNCTION

[0x00535670]> ii-?
255
[0x00535670]> ii-Disk
[0x00535670]> ii-Drive
ordinal=024 plt=0x00702654 bind=NONE type=FUNC name=KERNEL32.dll_GetDriveTypeA
[0x00535670]>
LET'S SCRIPT SOME DOCUMENTATION FETCHER FOR R2

```bash
jvoisin@kaa 18:11 ~ cat .config/radare2/radare2rc
$winapi=./bash /home/jvoisin/.config/radare2/winapi.sh
jvoisin@kaa 18:11 ~ cat /home/jvoisin/.config/radare2/winapi.sh
curl https://source.winehq.org/WineAPI/${1}.html 2>/dev/null | grep DESCRIPTION -A 1 | tail -n '+2' | sed -e 's/\^[^>]*//g'
jvoisin@kaa 18:11 ~ r2 -
    -- WASTED
[0x00000000]> $winapi GetDriveTypeW
Returns the type of the disk drive specified. If root is NULL the root of the current directory is used.
[0x00000000]> 
```
You’ve got this one in your .radare2rc in the VM
Your turn!

· Find where `GetDriveTypeA` is called
Your turn!

- Find where `GetDriveTypeA` is called
- It’s likely an analysis command, about `xref` to something
Your turn!

- Find where `GetDriveTypeA` is called
- It’s likely an analysis command, about `xref to` something
- There are two locations:
Your turn!

- Find where `GetDriveTypeA` is called
- It’s likely an analysis command, about `xref` to something
- There are two locations:
  - `0x4d65f6`
  - `0x5352ee`
Your turn!

- Find where `GetDriveTypeA` is called
- It’s likely an analysis command, about `xref` to something
- There are two locations:
  - `0x4d65f6`
  - `0x5352ee`
Your turn!

- Find where `GetDriveTypeA` is called
- It’s likely an analysis command, about `xref` to something
- There are two locations:
  - `0x4d65f6`
  - `0x5352ee`
- In what function do they belong?
Your turn!

- Find where `GetDriveTypeA` is called
- It’s likely an analysis command, about `xref` to something
- There are two locations:
  - `0x4d65f6`
  - `0x5352ee`
- In what function do they belong?
- Still in analysis, function related, about information
Your turn!

- Find where `GetDriveTypeA` is called
- It’s likely an analysis command, about `xref` to something
- There are two locations:
  - `0x4d65f6`
  - `0x5352ee`
- In what function do they belong?
- Still in analysis, function related, about information
  - `afi 0x4d65f6`
Your turn!

- Find where GetDriveTypeA is called
- It’s likely an analysis command, about xref to something
- There are two locations:
  - 0x4d65f6
  - 0x5352ee
- In what function do they belong?
- Still in analysis, function related, about information
  - afi 0x4d65f6
  - afi 0x5352ee
Your turn!

- 0x4d65f6 is called from two locations:
Your turn!

- 0x4d65f6 is called from two locations:
  - 0x004d6550

0x4d65f6 is the cd-check routine!
Your turn!

- **0x4d65f6** is called from two locations:
  - **0x004d6550**
  - **0x004ab1aa**
Your turn!

- **0x4d65f6** is called from two locations:
  - **0x004d6550**
  - **0x004ab1aa**

- Which one is the relevant one? (check with VV)
Your turn!

- 0x4d65f6 is called from two locations:
  - 0x004d6550
  - 0x004ab1aa

- Which one is the relevant one? (check with VV)
- 0x004d6550 is the cd-check routine!
1. Reopen the binary in write mode with oo+
2. Hardcode a return value for fcn.0x004d6550
3. Play the game without the CD!
File Empires.exe reopened in read-write mode

"wa mov eax, 1 ; ret 4"

Written 8 bytes (mov eax, 1 ; ret 4) = wx b801000000c20400
∙ Having no CD reader sucks,
∙ Age of Empire is cool,
∙ So is radare2.
Radare2 is nice.
You should use it.
RESOURCES

- Github repo
- Official website
- The r2 blog
- The r2 book
- Twitter