Kingdom of Saudi Arabia **Ministry of Education** **University of Jeddah** **College of Science and Computer Engineering**		**المملكة العربية السعودية** **وزارة التعليم** **جامعة جدّة** **كلية علوم و هندسة الحاسب**

CCCY432 – Reverse Engineering and Malware Analysis

Lab 6 – Unpacking Process Injection Code Using Debugger – part 2

Due Date: 3 nov 2024 11:00PM

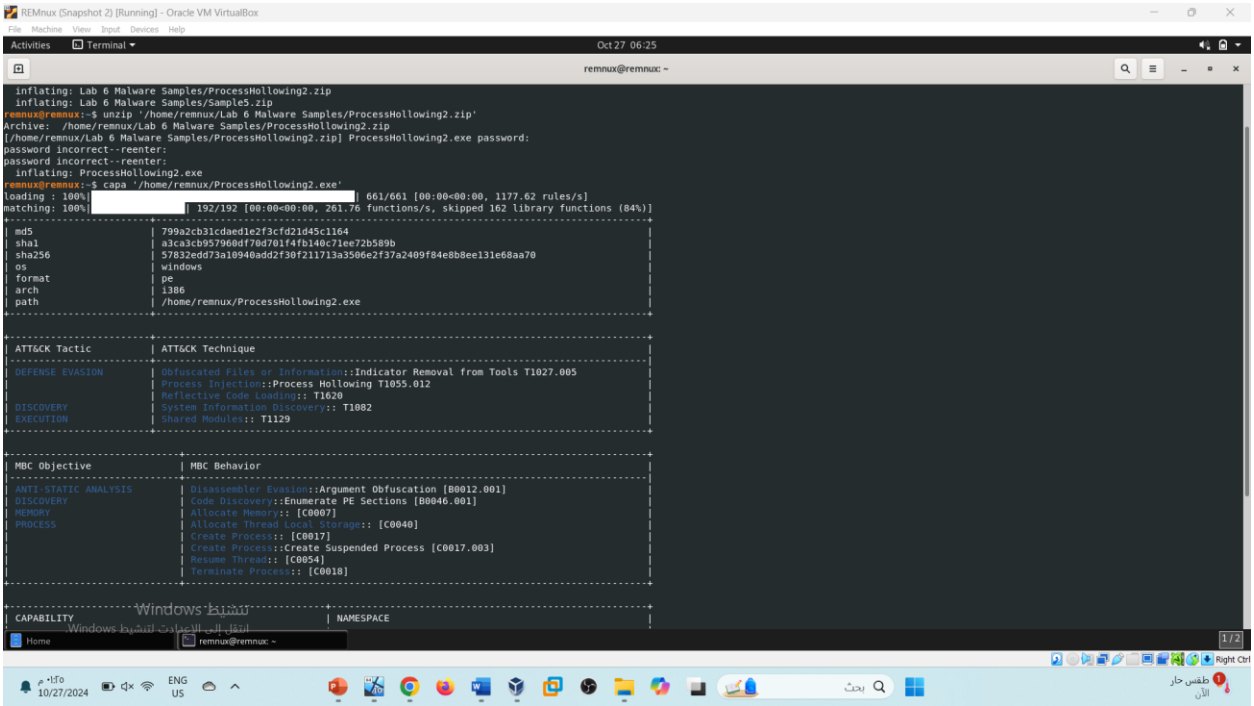
Lara Sami Alofi

2110886

Y

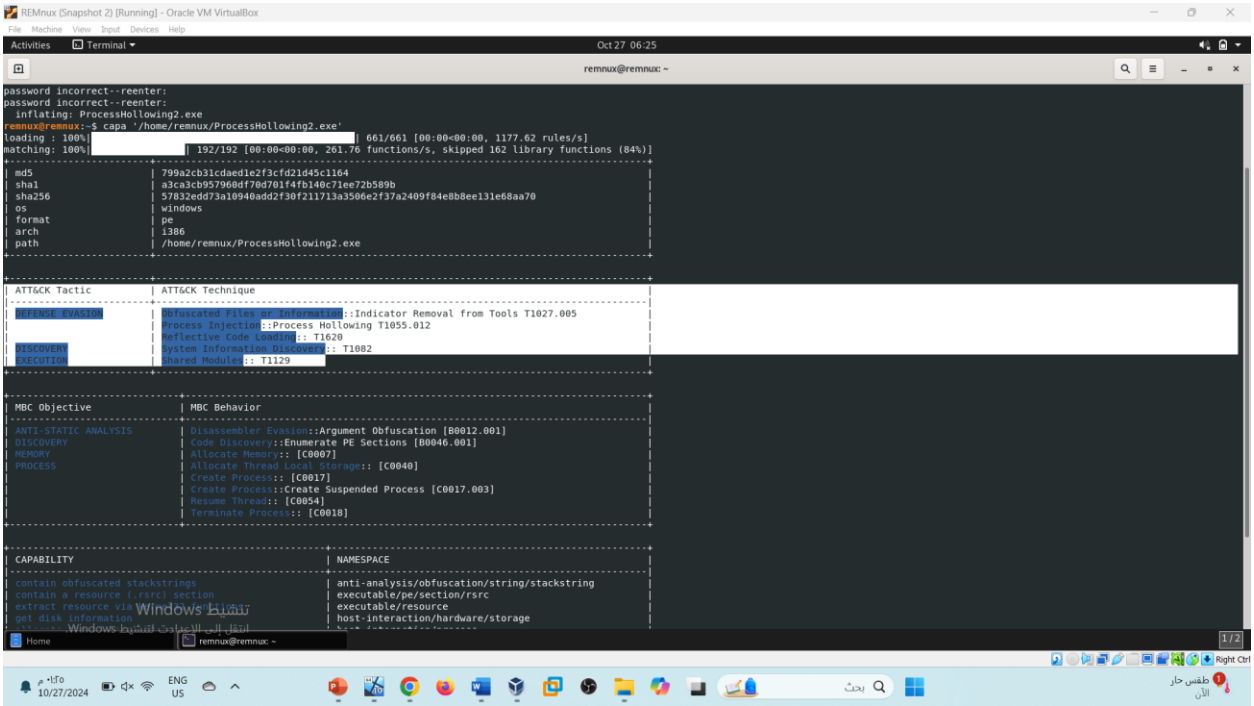
Task 4: Recognizing Process Hollowing technique in an executable:

1. In this task, we are going to investigate and recognize process hollowing pattern in the malware sample using Process_Hollwoing2.exe.



2. Follow the steps from Remnux capa tool and take screenshots of the following:

a. Take screenshot the ATT&CK Techniques of the malware in **your** Windows Machine



b. Take screenshot of the API details of the suspended process in **your** Windows Machine

REMnux (Snapshot 2) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Oct 27 06:27

remnux@remnux: ~

```
md5                     799a2cb31cdaed1e2f3cfd21d45c1164
sha1                    a3ca3cb957960df70d701f4fb140c71ee72b589b
sha256                  57832edd73a10940add2f30f211713a3506e2f37a2409f84e8b8ee131e68aa70
path                    /home/remnux/ProcessHollowing2.exe
timestamp               2024-10-27T06:26:37.256247
capa version            v3.2.0-0-gd9d72ad
os                      windows
format                  pe
arch                    i386
extractor               VivisectFeatureExtractor
base address            0x400000
rules                   /tmp/_MEIeKA9KP/rules
function count          30
library function count   162
total feature count      2617

contain obfuscated stackstrings
namespace  anti-analysis/obfuscation/string/stackstring
author     moritz.raabe@mandiant.com
scope      basic block
att&ck     Defense Evasion::Obfuscated Files or Information::Indicator Removal from Tools [T1027.005]
mbc        Anti-Static Analysis::Disassembler Evasion::Argument Obfuscation [B0012.001]
examples   Practical Malware Analysis Lab 16-03.exe_:0x4013D0
basic block @ 0x4010B0 in function 0x4010B0
  characteristic: stack string @ 0x4010B0

contain a resource (.rsrc) section
namespace  executable/pe/section/rsrc
author     moritz.raabe@mandiant.com
scope      file
examples   A933A1A402775CFA94B6BEE0963F4B46:0x41fd25
section: .rsrc @ 0x410000

extract resource via kernel32 functions
namespace  executable/resource
author     william.ballenthin@mandiant.com
scope      function
examples   BF88E1BD4A3BDE10B419A622278F1FF7:0x401000, Practical Malware Analysis Lab 01-04.exe_:0x4011FC, 563653399B82CD443F120ECEFF836EA3678D4CF11D9B351BB737573C2D856299:0x140001ABA
function @ 0x401000
  or:
    and:
      or:
        api: kernel32.LoadResource @ 0x401028
        api: kernel32.LockResource @ 0x401034
    optional:
```

Home remnux@remnux: ~ 1 / 2

Right Ctrl

10/27/2024 ٠٦:٢٧ م ENG US

REMnux (Snapshot 2) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Oct 27 06:28

remnux@remnux: ~

```
function @ 0x405512
  or:
    api: kernel32.TlsAlloc @ 0x405512

create process on Windows
namespace  host-interaction/process/create
author     moritz.raabe@mandiant.com
scope      basic block
mbc        Process::Create Process [C0017]
examples   9324D1A8AE37A36AE560C37448C9705A:0x406DB0, Practical Malware Analysis Lab 01-04.exe_:0x4011FC
basic block @ 0x402130 in function 0x402130
  and:
    os: windows
    or:
      api: kernel32.CreateProcess @ 0x4021AE

create process suspended
namespace  host-interaction/process/create
author     william.ballenthin@mandiant.com
scope      basic block
mbc        Process::Create Process::Create Suspended Process [C0017.003]
examples   Practical Malware Analysis Lab 03-03.exe_:0x4010EA
basic block @ 0x402130 in function 0x402130
  and:
    or:
      number: 0x4 = CREATE_SUSPENDED @ 0x40218C
    or:
      api: kernel32.CreateProcess @ 0x4021AE

allocate RWX memory (2 matches)
namespace  host-interaction/process/inject
author     moritz.raabe@mandiant.com
scope      basic block
mbc        Memory::Allocate Memory [C0007]
examples   Practical Malware Analysis Lab 03-03.exe_:0x4010EA, 563653399B82CD443F120ECEFF836EA3678D4CF11D9B351BB737573C2D856299:0x140001ABA
basic block @ 0x401000 in function 0x401000
  and:
    match: allocate memory @ 0x401000
      or:
        api: kernel32.VirtualAlloc @ 0x401077
    number: 0x40 = PAGE_EXECUTE_READWRITE @ 0x401068
basic block @ 0x4021EE in function 0x402130
  and:
    match: allocate memory @ 0x4021EE
      or:
```

Recognizing Process Hollowing te...

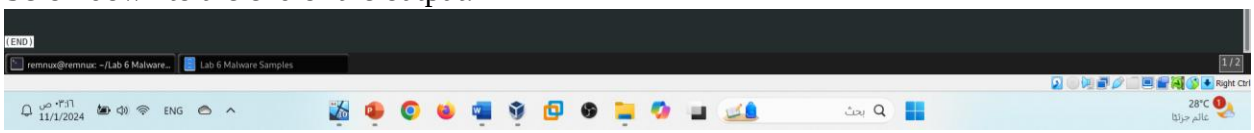
Home remnux@remnux: ~ 1 / 2

Right Ctrl

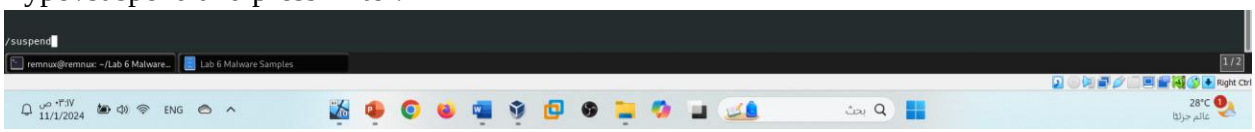
10/27/2024 ٠٦:٢٨ م ENG US

c. From the output of capa, what is the address of kernel32.CreateProcess?

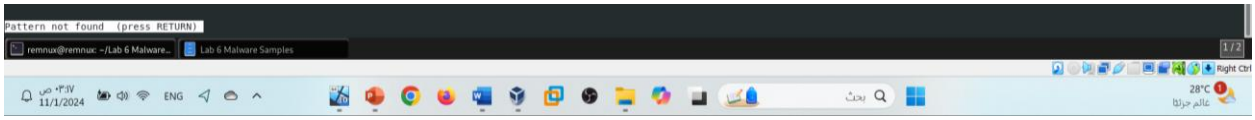
1- Run the command: capa -vv /home/remnux/ProcessHollowing2.exe | less
2- Scroll down to the end of the output.



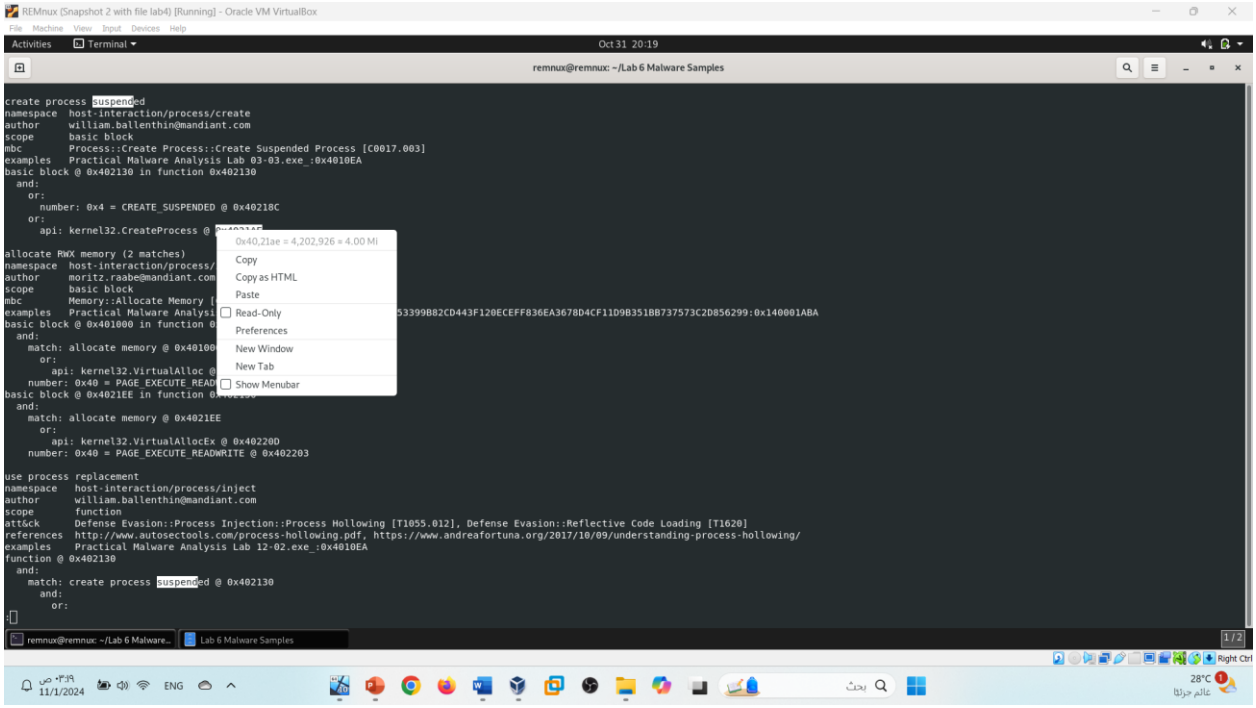
3- Type /suspend and press Enter.



4- Press Enter



5- Scroll up to locate and copy the address of CreateProcessA.

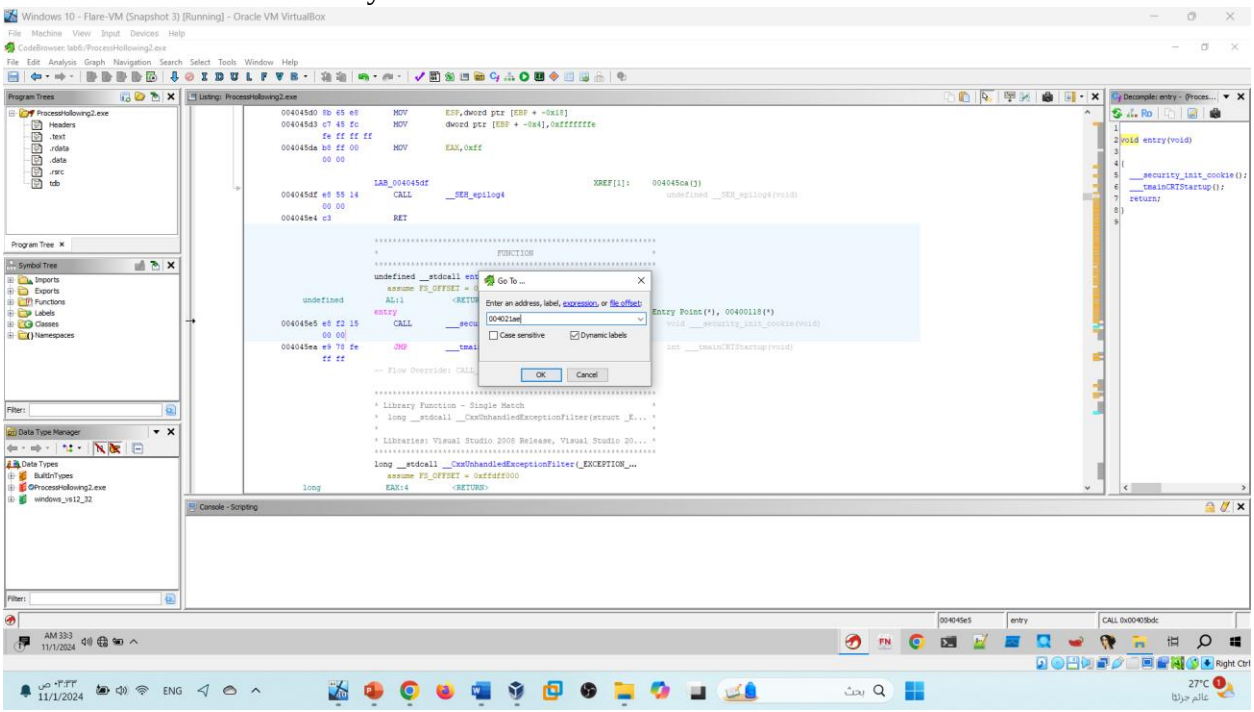


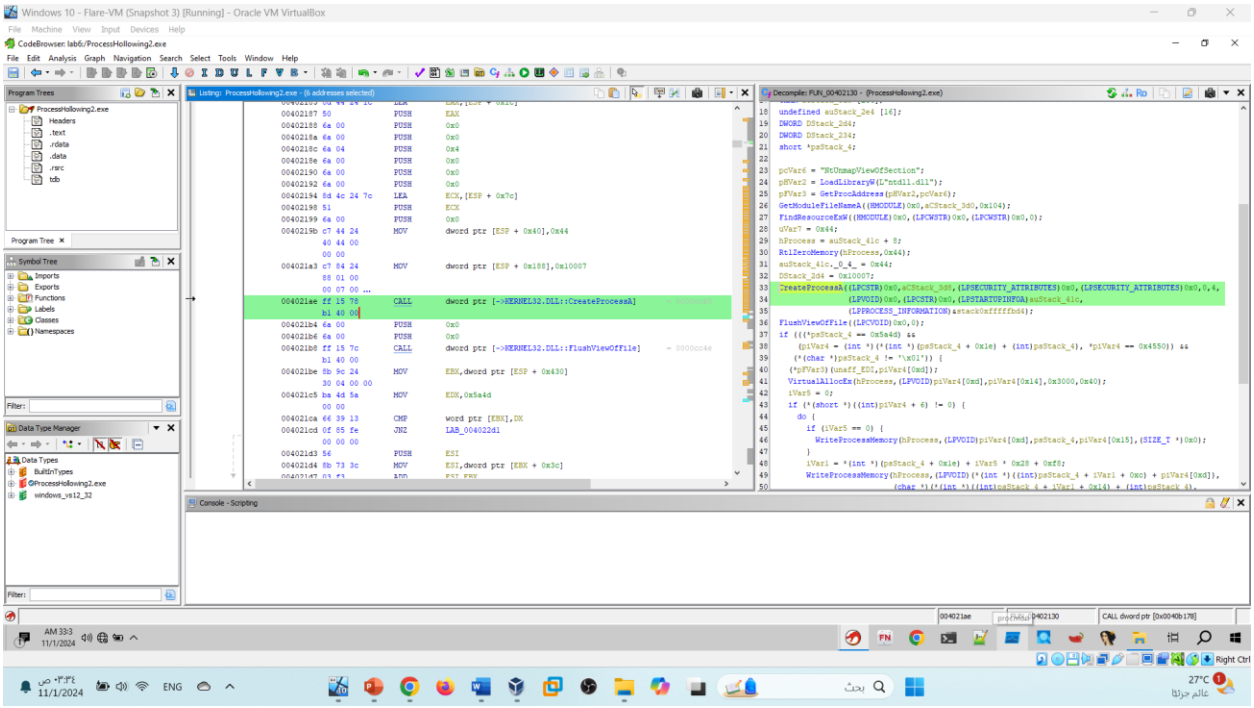
The CreateProcessA function from kernel32.dll is located at 0x4021ae in this disassembly.

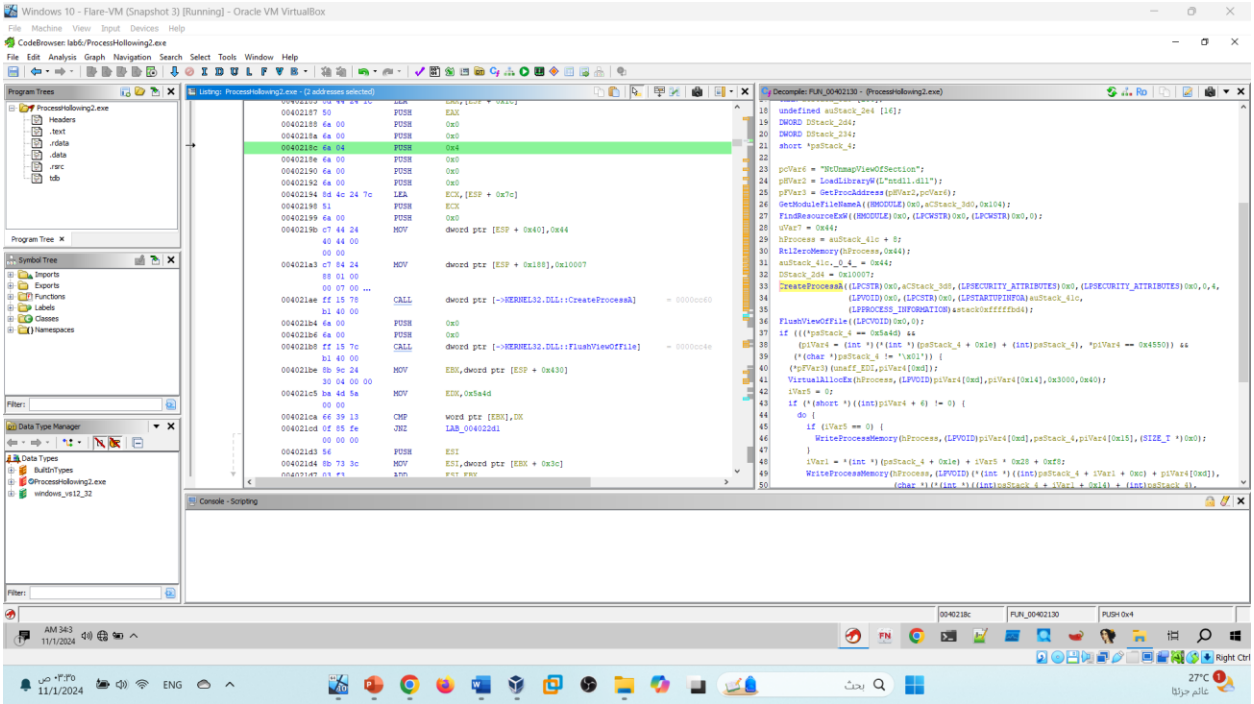
d. To write the instruction at 0x40218c in Flare-VM:

1- Import the file into Ghidra and start the analysis.

2- Press Ctrl + G to search by address.







The instruction at address 0x40218c is PUSH 0x4.