


<b>Kingdom of Saudi Arabia Ministry of Education University of Jeddah College of Science and Computer Engineering</b>	 جامعة جدة University of Jeddah	<b>المملكة العربية السعودية وزارة التعليم جامعة جدة كلية علوم و هندسة الحاسب</b>
---	---	--

**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\_Hollowing2.exe.

```
REMnux (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Oct 27 06:25
remux@remnux:~$
Inflating: Lab 6 Malware Samples/ProcessHollowing2.zip
Inflating: Lab 6 Malware Samples/Sample5.zip
remux@remnux:~$ unzip -j /home/remnux/Lab 6 Malware Samples/ProcessHollowing2.zip
Archives: /home/remnux/Lab 6 Malware Samples/ProcessHollowing2.zip
/home/remnux/Lab 6 Malware Samples/ProcessHollowing2.zip ProcessHollowing2.exe password:
password incorrect--reenter:
password incorrect--reenter:
Inflating: ProcessHollowing2.exe
remux@remnux:~$ capa '/home/remnux/ProcessHollowing2.exe'
loading: 100% [REDACTED] 661/661 [00:00:00:00, 1177.62 rules/s]
matching: 100% [REDACTED] 192/192 [00:00:00:00, 261.76 functions/s, skipped 162 library functions (84%)]
-----
md5 | 799a2cb31cdae1d2f3cf021d45c1164
sha1 | a3ca3cb95796df7d0701f4fb140c71ee72b589b
sha256 | 57832edd73a10940add2f30f211713a3506e2f37a2409f84e8b8ee131e68aa70
os | windows
format | pe
arch | i386
path | /home/remnux/ProcessHollowing2.exe
-----
ATT&CK Tactic | ATT&CK Technique
-----
DEFENSE EVASION | Obfuscated Files or Information::Indicator Removal from Tools T1027.005
| Process Injection::Process Hollowing T1055.012
| Reflective Code Loading:: T1060
DISCOVERY | System Information Discovery:: T1082
EXECUTION | Shared Modules:: T1129
-----
MBC Objective | MBC Behavior
-----
API STATIC ANALYSIS | Disassembler Extension::Argument Obfuscation [B0012.001]
DISCOVERY | Code Discovery::Enumerate PE Sections [B0046.001]
MEMORY | Allocate Memory:: [C0007]
PROCESS | Allocate Thread Local Storage:: [C0040]
| Create Process:: [C0017]
| Create Process::Create Suspended Process [C0017.003]
| Resume Thread:: [C0054]
| Terminate Process:: [C0018]
-----
CAPABILITY Windows | Windows
-----
CAPABILITY Windows | NAMESPACE
-----
Home remux@remnux:~$
```

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

The image shows a Windows 10 desktop environment. In the foreground, a Windows Security notification is displayed, indicating that Windows Defender detected a potentially unwanted application (PUA) named 'ProcessHollowing2.exe' and blocked it. The notification includes details about the file's origin (Microsoft Store), its size (1.1 MB), and its hash. Below the notification, a terminal window is open, showing the execution of the 'ProcessHollowing2.exe' process. The terminal output displays various system information, including the process's name, path, and architecture. The desktop background is a Windows 10 wallpaper, and the taskbar at the bottom shows several open applications, including the Start menu, File Explorer, and the terminal window.

- 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 799a2cb31cdaed1e2f3cfd21d045c1164
sha1 33ca3cb579980d176d781f4b146c71ee72b580b
sha256 57832edd73a10940add2f30f211713a3506e2f37a2409f84e8b8ee131e68aa70
path /home/remnux/ProcessHollowing2.exe
timestamp 2024-10-27T06:26:37.256247
cpa version v3.2.0-0-gd9d72ad
os windows
format pe
arch i386
extractor VivisectFeatureExtractor
base address 0x400000
rules /tmp/.MEtEKa9KP/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
attack Defense Evasion::Obfuscated Files or Information::Indicator Removal from Tools [T1027.005]
mbc Anti-Static Analysis::Disassembler Evasion::Argument Obfuscation [00012.001]
examples Practical Malware Analysis Lab 10-03.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 A933A1A02775CFA94B6EE0963F4B46:0x41fd25
section: .rsrc @ 0x410000

extract resource via kernel32 functions
namespace executable/resource
author william.ballenthin@mandiant.com
scope function
examples BFB8E1D04A38DE10B419A62227B1FF7:0x401000, Practical Malware Analysis Lab 01-04.exe :0x4011FC, 5636533998B2CD443F120CEFF836EA3678D4CF1D983518B73753C2D856299:0x140001ABA
function @ 0x401000
or:
or:
api: kernel32.LoadResource @ 0x401028
api: kernel32.LockResource @ 0x401034
optional:
تنشيط Windows
انتقل إلى الإعدادات لتنشيط Windows
remnux@remnux ~
1/2
```

```
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

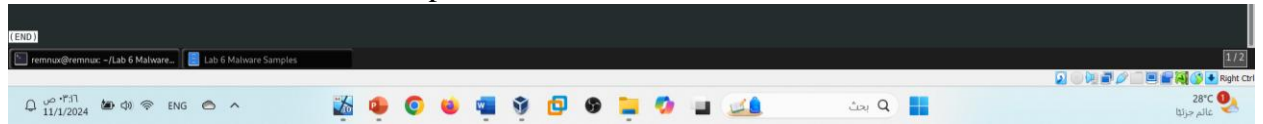
create process on Windows
namespace host-interaction/process/create
author moritz.raabe@mandiant.com
scope basic block
mbc Process::Create Process [C0017]
examples 9324018AE37A36AE560C37440C9705A:0x4060B0, Practical Malware Analysis Lab 01-04.exe :0x4011FC
basic block @ 0x402130 in function 0x402130
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
Recognizing Process Hollowing te...

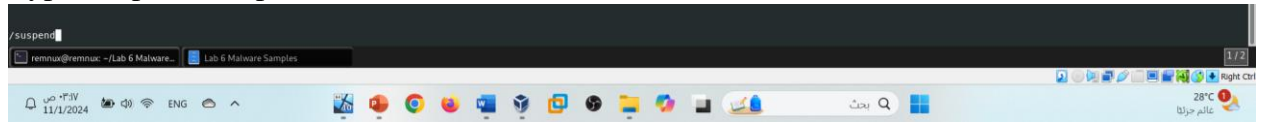
allocate Rwx memory (2 matches)
namespace host-interaction/process/inject
author moritz.raabe@mandiant.com
scope basic block
mbc Memory::Allocate Memory [C0007]
examples Practical Malware Analysis Lab 03-03.exe :0x4010EA, 5636533998B2CD443F120CEFF836EA3678D4CF1D983518B73753C2D856299:0x140001ABA
basic 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
تنشيط Windows
انتقل إلى الإعدادات لتنشيط Windows
remnux@remnux ~
1/2
```

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

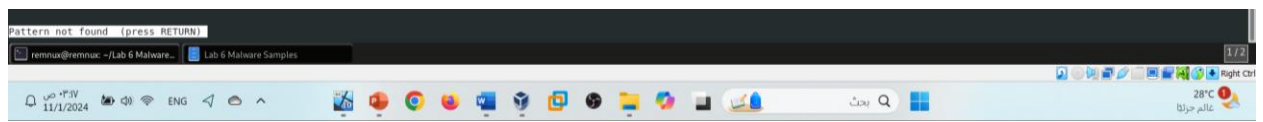
- 1- Run the command: `capa -vv /home/remnux/ProcessHollowing2.exe | less`
- 2- Scroll down to the end of the output.



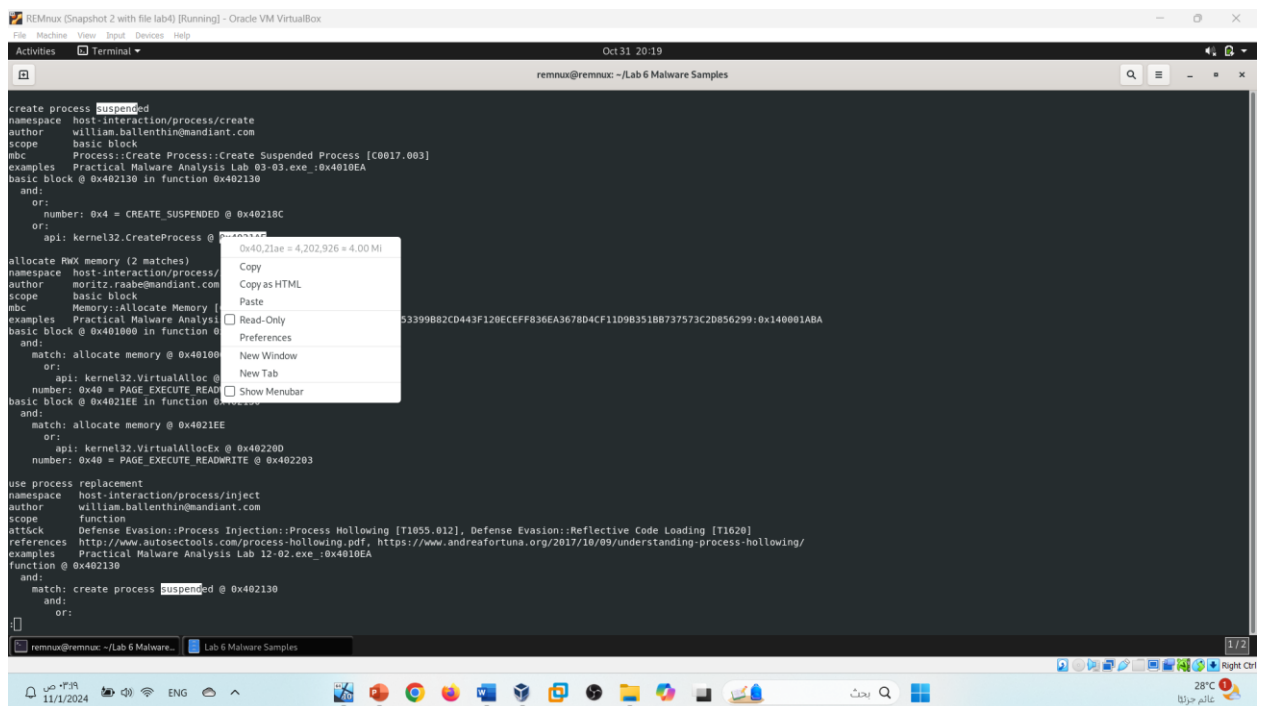
- 3- Type `/suspend` and press Enter.



- 4- Press Enter



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

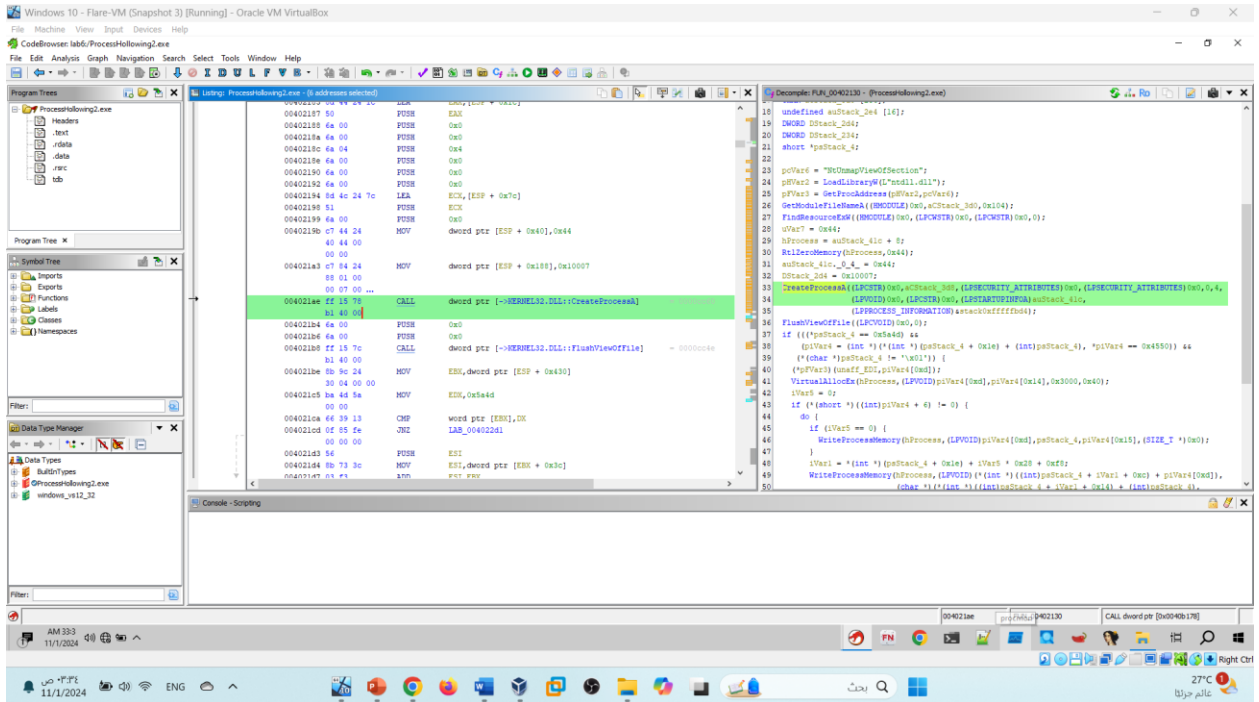
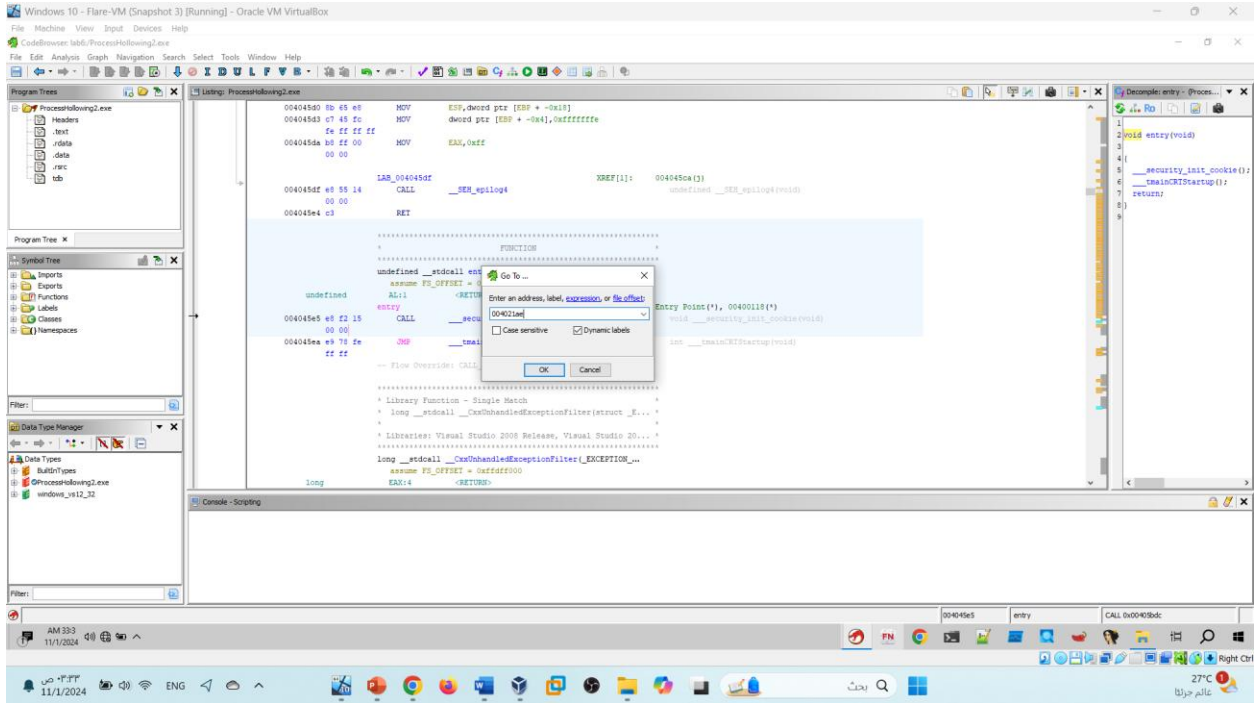


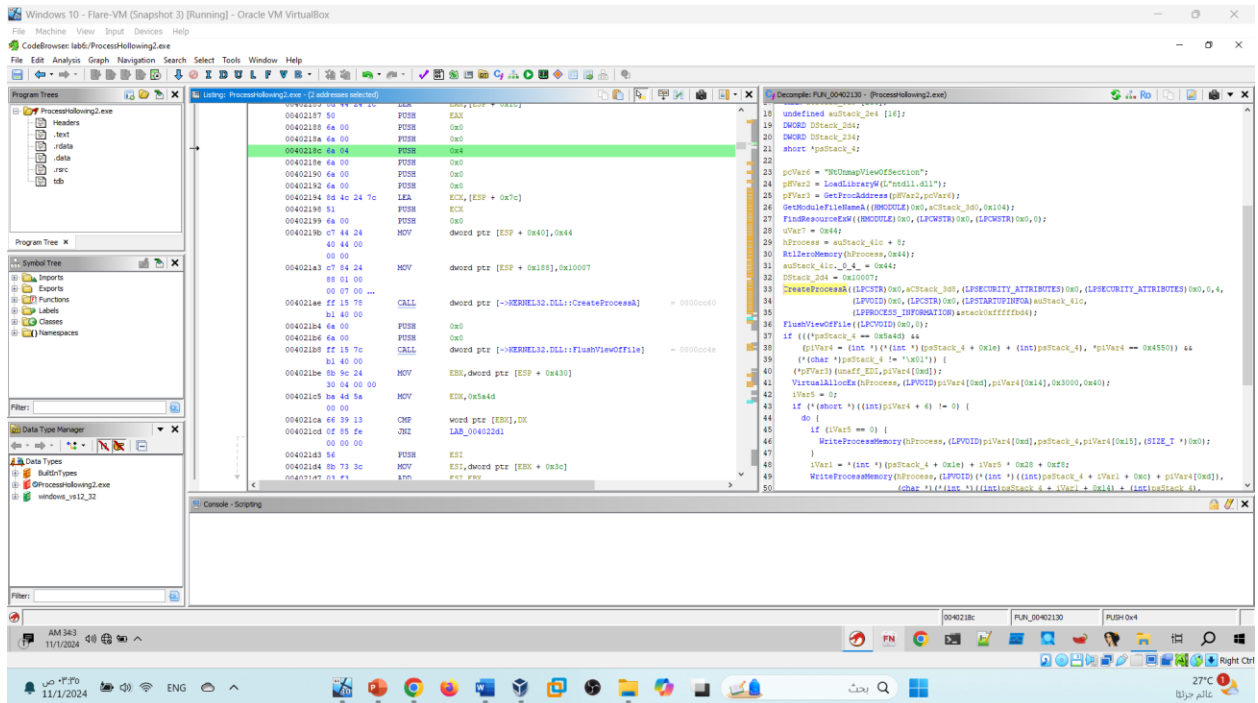
The CreateProcessA function from kernel32.dll is located at 0x4021ae in this disassembly.

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.