

Hgame-Vidar 2021 week4

20-啥也不会-小九

MISC

Akira之瞳-1

下载压缩包解压得后缀为raw的文件，起初认为是照片

一解压正好1.0G 拖到PS里也没看出什么名堂

以“raw”“dump”“ctf”为关键词搜到内存取证

搜索“内存取证”搜到volatility的使用指南<https://www.cnblogs.com/jssi/p/13762308.html>

volatility -f important_work.raw imageinfo获取系统信息

volatility -f important_work.raw --profile=Win7SP1x64 pslist查看所有进程

```
PS D:\Desktop\tools\volatility_2.6_win64_standalone> .\volatility -f 1.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
0xfffffa800cd34040	System	4	0	158	487	-----	0	2021-02-18 09:45:38 UTC+0000
0xfffffa800d975b30	smss.exe	364	4	2	44	-----	0	2021-02-18 09:45:38 UTC+0000
0xfffffa800d88f9d0	csrss.exe	456	420	9	539	0	0	2021-02-18 09:45:41 UTC+0000
0xfffffa800cd52060	wininit.exe	500	420	4	95	0	0	2021-02-18 09:45:41 UTC+0000
0xfffffa800e139b30	csrss.exe	520	508	11	235	1	0	2021-02-18 09:45:41 UTC+0000
0xfffffa800e182910	services.exe	568	500	14	283	0	0	2021-02-18 09:45:41 UTC+0000
0xfffffa800e193910	lsass.exe	576	500	10	618	0	0	2021-02-18 09:45:41 UTC+0000
0xfffffa800e198b30	lsmon.exe	584	500	11	167	0	0	2021-02-18 09:45:42 UTC+0000
0xfffffa800e3b0060	winlogon.exe	680	508	7	139	1	0	2021-02-18 09:45:42 UTC+0000
0xfffffa800e3c4b30	svchost.exe	720	568	13	411	0	0	2021-02-18 09:45:42 UTC+0000
0xfffffa800e3e8060	vmtoolsd.exe	780	568	3	59	0	0	2021-02-18 09:45:42 UTC+0000
0xfffffa800e3fb3e0	svchost.exe	820	568	7	315	0	0	2021-02-18 09:45:42 UTC+0000
0xfffffa800e42bb30	svchost.exe	896	568	21	455	0	0	2021-02-18 09:45:42 UTC+0000
0xfffffa800e42a750	svchost.exe	940	568	23	487	0	0	2021-02-18 09:45:42 UTC+0000
0xfffffa800e445740	svchost.exe	968	568	44	900	0	0	2021-02-18 09:45:42 UTC+0000
0xfffffa800e479b30	audiocd.exe	180	896	6	149	0	0	2021-02-18 09:45:42 UTC+0000
0xfffffa800e49a890	svchost.exe	400	568	14	600	0	0	2021-02-18 09:45:42 UTC+0000
0xfffffa800e4bb3a0	svchost.exe	212	568	22	432	0	0	2021-02-18 09:45:43 UTC+0000
0xfffffa800e5f4410	spoolsv.exe	1184	568	17	360	0	0	2021-02-18 09:45:43 UTC+0000
0xfffffa800e614520	svchost.exe	1212	568	27	367	0	0	2021-02-18 09:45:43 UTC+0000
0xfffffa800e745b30	VGAAuthService.exe	1532	568	5	121	0	0	2021-02-18 09:45:44 UTC+0000
0xfffffa800e7bd060	vmtoolsd.exe	1584	568	11	285	0	0	2021-02-18 09:45:44 UTC+0000
0xfffffa800e84ab30	WmiPrvSE.exe	1848	720	11	202	0	0	2021-02-18 09:45:44 UTC+0000
0xfffffa800e832b30	dllhost.exe	1292	568	36	297	0	0	2021-02-18 09:45:45 UTC+0000
0xfffffa800e8fab30	svchost.exe	444	568	7	111	0	0	2021-02-18 09:45:45 UTC+0000
0xfffffa800e708960	dllhost.exe	2148	568	17	240	0	0	2021-02-18 09:45:45 UTC+0000
0xfffffa800e9524e0	msdtc.exe	2240	568	16	173	0	0	2021-02-18 09:45:45 UTC+0000
0xfffffa800e994060	VSSVC.exe	2440	568	6	134	0	0	2021-02-18 09:45:46 UTC+0000
0xfffffa800eae1b30	WmiPrvSE.exe	2692	720	12	307	0	0	2021-02-18 09:46:04 UTC+0000
0xfffffa800eb54950	WmiApSrv.exe	2800	568	7	129	0	0	2021-02-18 09:46:05 UTC+0000
0xfffffa800eb8b630	taskhost.exe	2960	568	10	196	1	0	2021-02-18 09:46:50 UTC+0000
0xfffffa800ec09b30	dwm.exe	1540	940	7	131	1	0	2021-02-18 09:46:51 UTC+0000
0xfffffa800ec12b30	explorer.exe	2232	3064	32	713	1	0	2021-02-18 09:46:51 UTC+0000
0xfffffa800ecaf210	vmtoolsd.exe	1364	2232	5	81	1	0	2021-02-18 09:46:54 UTC+0000
0xfffffa800ec313e0	vmtoolsd.exe	1268	2232	9	180	1	0	2021-02-18 09:46:54 UTC+0000
0xfffffa800e5ab460	taskmgr.exe	2780	680	12	144	1	0	2021-02-18 09:46:59 UTC+0000
0xfffffa800e5c6b30	SearchIndexer.exe	1252	568	13	647	0	0	2021-02-18 09:47:00 UTC+0000
0xfffffa800ed50b30	wmpnetwk.exe	2572	568	13	251	0	0	2021-02-18 09:47:00 UTC+0000
0xfffffa800ed2eb30	svchost.exe	2596	568	13	182	0	0	2021-02-18 09:47:00 UTC+0000
0xfffffa800f246670	SearchProtocolHost.exe	736	1252	7	245	1	0	2021-02-18 09:47:11 UTC+0000
0xfffffa800f248060	SearchFilterHost.exe	2552	1252	5	101	0	0	2021-02-18 09:47:11 UTC+0000
0xfffffa800f263b30	important_work	1092	2232	1	16	1	1	2021-02-18 09:47:15 UTC+0000
0xfffffa800f260060	conhost.exe	1372	520	2	63	1	0	2021-02-18 09:47:16 UTC+0000
0xfffffa800f29fb30	cmd.exe	1340	1092	1	29	1	1	2021-02-18 09:47:16 UTC+0000
0xfffffa800f13590	dllhost.exe	3128	720	6	102	1	0	2021-02-18 09:47:21 UTC+0000
0xfffffa800f2ba750	dllhost.exe	3184	720	6	99	0	0	2021-02-18 09:47:22 UTC+0000
0xfffffa800f277b30	DumpIt.exe	3216	2232	2	75	1	1	2021-02-18 09:47:22 UTC+0000
0xfffffa800edc6240	conhost.exe	3224	520	2	61	1	0	2021-02-18 09:47:22 UTC+0000

发现名为important_work的进程 与压缩包以及镜像同名

volatility -f important_work1.raw --profile=Win7SP1x64 memdump -p 1092 -D D:\desktop 转存为dmp文件

```
PS D:\Desktop\tools\volatility_2.6_win64_standalone> .\volatility -f l.raw --profile=Win7SP1x64 memdump -p 1092 -D D:\desktop
Volatility Foundation Volatility Framework 2.6
*****
Writing important_work [ 1092] to 1092.dmp
PS D:\Desktop\tools\volatility_2.6_win64_standalone>
```

得到1092.dmp后发现默认的打开方式是bandizip

打开发现Password is sha256(login_password)

volatility -f important_work.raw --profile=Win7SP1x64 hashdump timeliner提取密码

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Genga03:1001:aad3b435b51404eeaad3b435b51404ee:84b0d9c9f830238933e7131d60ac6436:::
PS D:\Desktop\tools\volatility_2.6_win64_standalone>
```

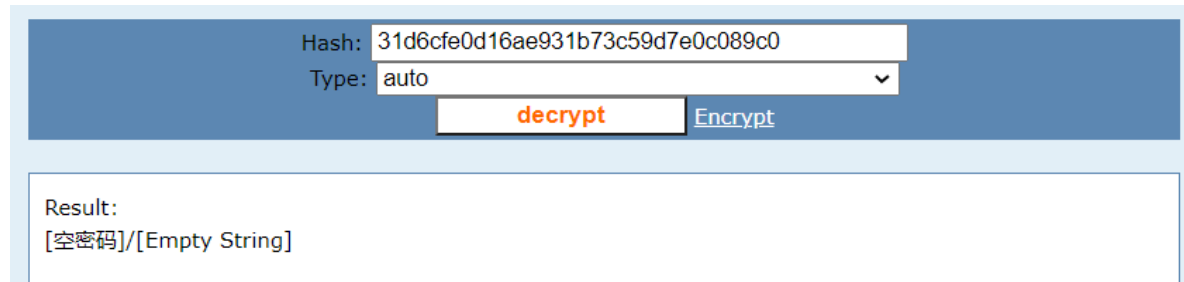
猜测是某种hash

搜索“hash” “windows密码”找到<https://www.cnblogs.com/feizianquan/p/10899098.html>

博客末尾详述了这串hash的结构和用法

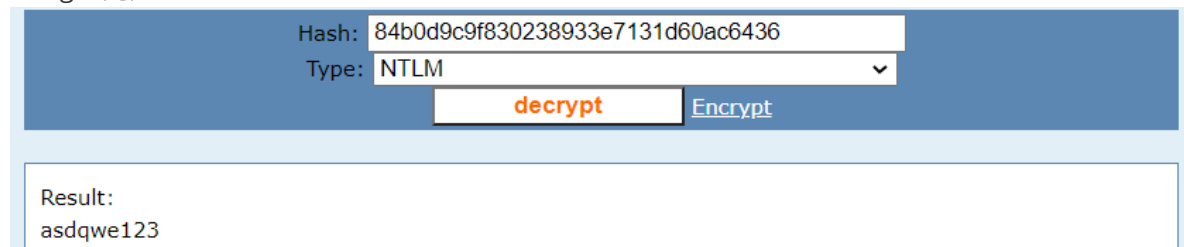
将三个用户的NT-HASH值丢到cmd5.org里

administrator和guest都是空密码



Hash: 31d6cfe0d16ae931b73c59d7e0c089c0
Type: auto
decrypt Encrypt
Result:
[空密码]/[Empty String]

Genga3则为



Hash: 84b0d9c9f830238933e7131d60ac6436
Type: NTLM
decrypt Encrypt
Result:
asdqwe123

将asdqwe123丢到sha256在线转换器里得

20504cdfddaad0b590ca53c4861edd4f5f5cf9c348c38295bd2dbf0e91bca4c3

解压得两张看起来完全一致 除了大小 参数也完全一致

week1搜图片隐写的时候对双图隐写这个分支有点印象

搜索“双图隐写”找到 <https://blog.xiafeng2333.top/ctf-16/>

博客中提到异或、盲水印、容差三种方法

结合blind这个图片名及两张图片的特点确定为盲水印

<https://github.com/chishaxie/BlindWaterMark>

找到python脚本

python bwm.py decode blind.png src.png wm.png

报错提示缺了cv2

pip命令装了半天装不上 想起来有清华源

得到盲水印 艰难地辨认出flag (1 和 l 真的太痛苦了)

