暗藏玄机[SOLVED]

Description

要开学了，要开学了（悲）

URL http://plqfgjy5a.bkt.clouddn.com/%E5%BC%80%E5%AD%A6.zip

Base Score 150

Now Score 150

User solved 34

盲水印，找个对的脚本。·

Warmup[SOLVED]

Description

提交管理员密码的sha256，自己补上格式hgame{}

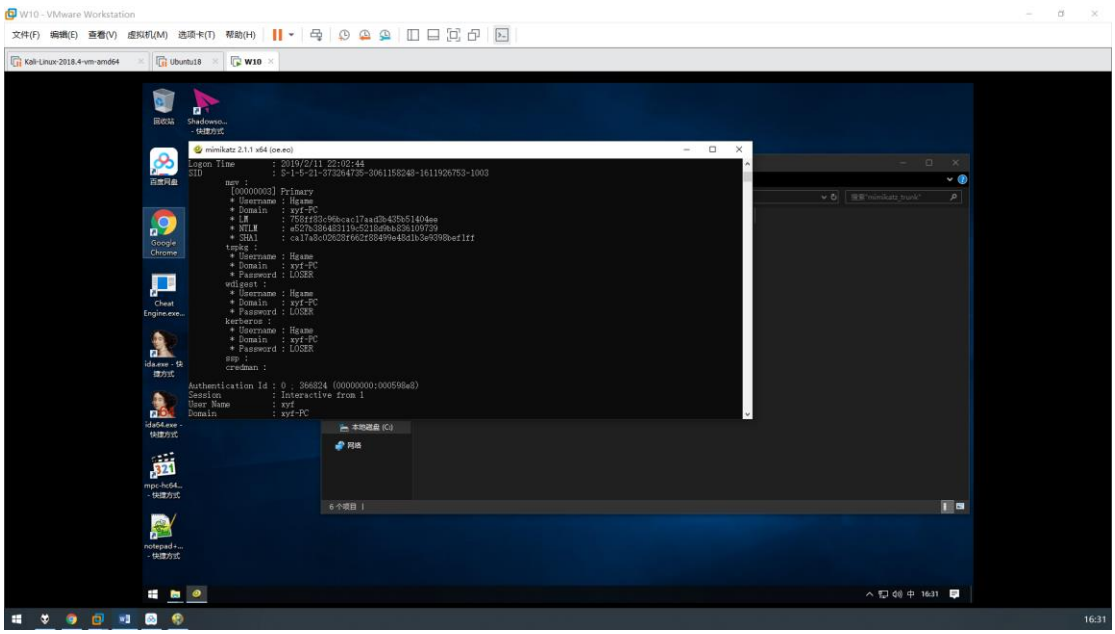
URL http://pmsw8b6r5.bkt.clouddn.com//ea72c72ba8808ccc22ca7f0fac63cfcb/1.zip

Base Score 100

Now Score 100

User solved 25

Gif 改 dmp



Hash在线计算、md5计算、sha1计算、sha256计算、sha512计算

LOSER

计算

#	算法	结果	结果(大写)	长
1	md5	08677becdfac904ce9f45a6d5645a3e6	08677BECDFAC904CE9F45A6D5645A3E6	32
2	sha1	7f133b2b30980a528ae20efc8dbddc2afbd4eef9	7F133B2B30980A528AE20EFC8DBDDC2AFBD4EEF9	40
3	sha256	dd6dffcd56b77597157ac6c1beb514aa4c59d033098f806d88df89245824d3f5	DD6DFFCD56B77597157AC6C1BEB514AA4C59D033098F806D88DF89245824D3F5	64
4	sha512	6733c6f6c4264f27a678126f820aaa421ba9e15751f3d6c7275d71fbc89b79f4144b3d8b50fc272b4c20e79f979535f68ee25fb9e078a81464f2e2529f0efaa5	6733C6F6C4264F27A678126F820AAA421BA9E15751F3D6C7275D71FBC89B79F4144B3D8B50FC272B4C20E79F979535F68EE25FB9E078A81464F2E2529F0EFAA5	128
5	adler32	04920186	04920186	8
6	crc32	e535e525	E535E525	8

系统挂了，还有一个 coldown

就是你看那个文件辣么大，然后名字又有什么内存的，想想是 volatility，你打开 imageinfo 一下（就是我两个环境下出来的结果都不一样？）然后再—profile=（你出来那个系统）

通过 hivelist 来列出缓存在内存中的注册表有哪些（蜂巢）:

volatility -f xxx.xx –profile=xx.xx hivelist

如果你想获取内存中的系统密码，我们可以使用 hashdump 将它提取出来:

volatility -f xxx.xx –profile=xxx.xx hashdump -y（注册表 system 的 virtual 地址 ）-s（SAM 的 virtual 地址）

可以看到 hash 值都被 dump 出来了。

就是解 hash，xp 和 vista 即以上的加密方式不同。一个是 lm 一个是 ntlm。网上说 ntlm 以 ophcrack 破不了，其实不一定，但是基本上是解决不了的。用 hashcat，hashcat 在装 opencl 的时候很多教程都是错误的。叫你直接去英特尔的官网上下，但其实他已经改版了,你找不到的。SRB4.1_linux64 这个文件，你搜一下应该可以找到别人保存到文件。但是他这个密码也很坑，你单用 rockyou 也爆不出，单暴力也不行（就是普通的 ?d?l?u）这样的。自定义暴力，或者找本好点的弱口令字典。