hgame_2020_Week-3_Write-up

web

这周主要是看了看序列之争和二手市场两道题，但是都做到一半卡住了，好菜~

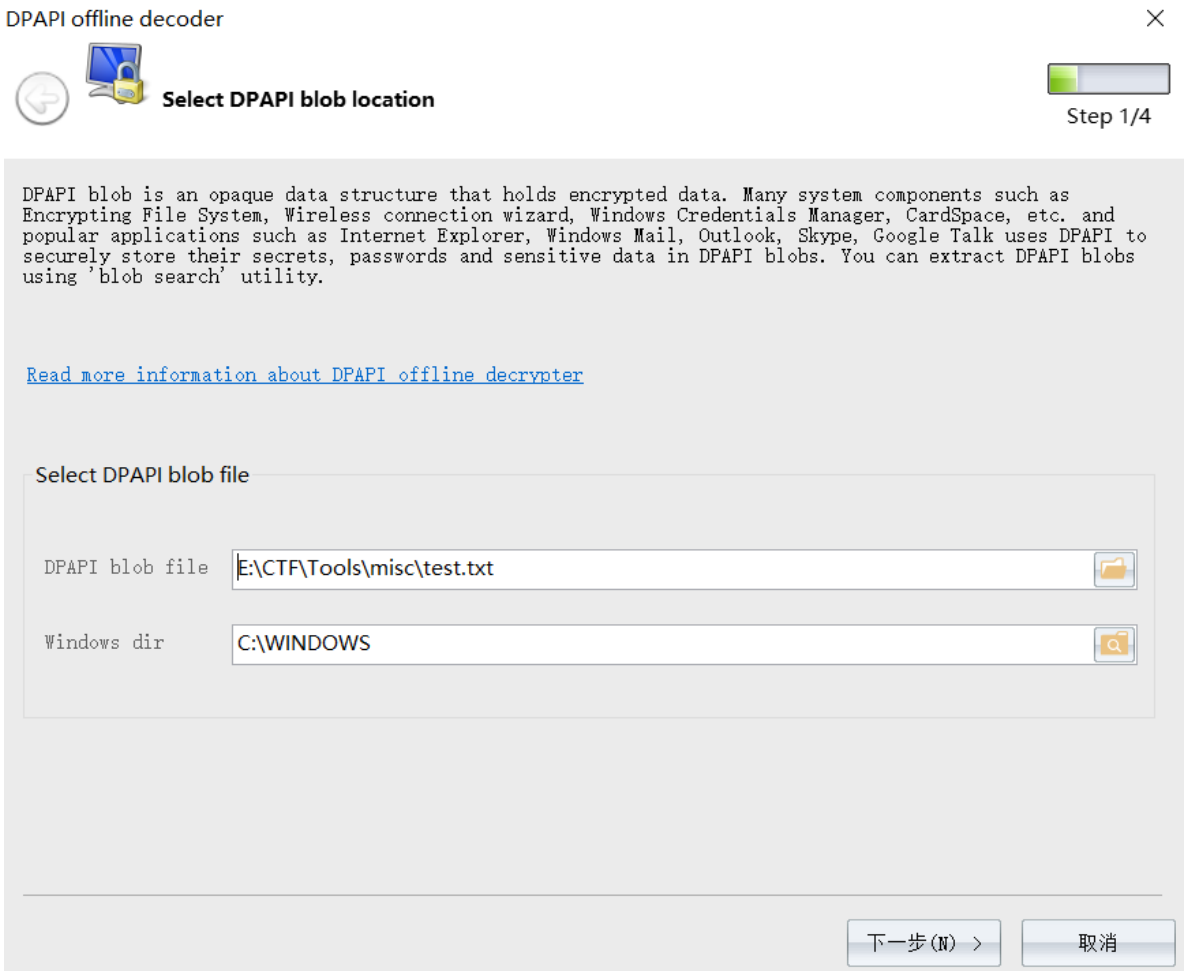
misc

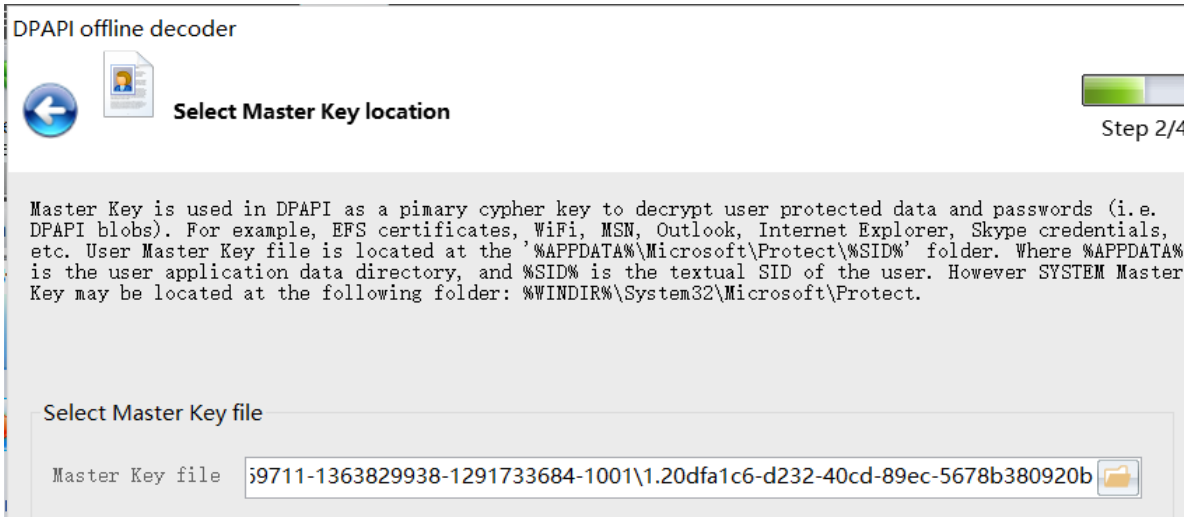
日常

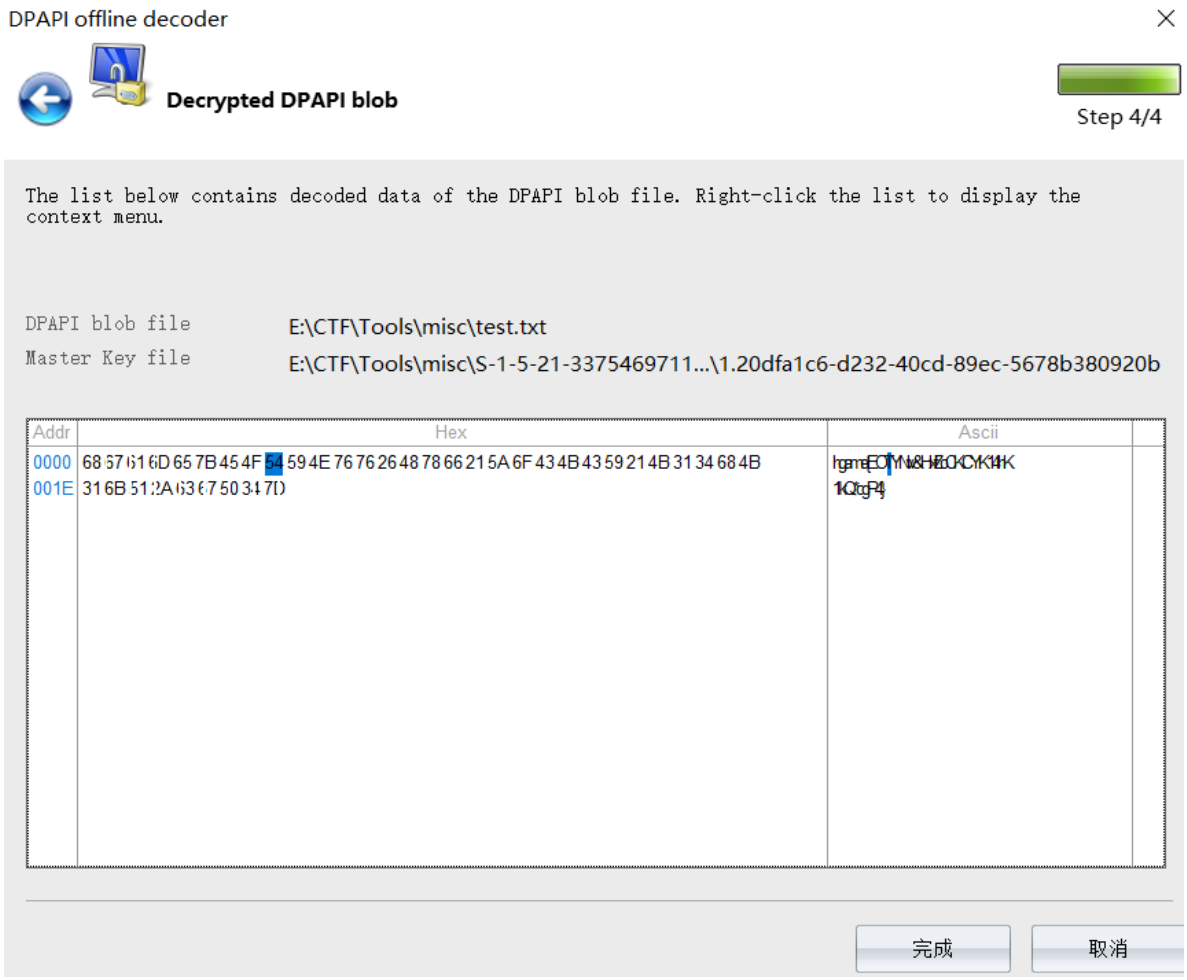
题目给了origin和blind两张图片，猜测是盲水印，解出来得到

VeraCrypt Password is X0YAlGDuZF$echCy

此外binwalk给的ogg文件又发现了一个container的容器，用VeraCrypt解密（注意容器不能放在系统盘解密）得到一个cookies以及一个mimikatz的日志，还有一个奇怪的S-1-5的文件夹，百度查询发现和3ctf的流量分析很像，之后的参考了 https://blog.csdn.net/yh1013024906/article/details/102952104，之后的password可以用日志中的NTLM解出。


DPAPI offline decoder
Select DPAPI blob location
Step 1/4
DPAPI blob is an opaque data structure that holds encrypted data. Many system components such as Encrypting File System, Wireless connection wizard, Windows Credentials Manager, CardSpace, etc. and popular applications such as Internet Explorer, Windows Mail, Outlook, Skype, Google Talk uses DPAPI to securely store their secrets, passwords and sensitive data in DPAPI blobs. You can extract DPAPI blobs using 'blob search' utility.
Read more information about DPAPI offline decrypter
Select DPAPI blob file
DPAPI blob file
E:\CTF\Tools\misc\test.txt
Windows dir
C:\WINDOWS
下一步(N) >
取消


DPAPI offline decoder
Select Master Key location
Step 2/4
Master Key is used in DPAPI as a pimary cypher key to decrypt user protected data and passwords (i.e. DPAPI blobs). For example, EFS certificates, WiFi, MSN, Outlook, Internet Explorer, Skype credentials, etc. User Master Key file is located at the '%APPDATA%\Microsoft\Protect\%SID%' folder. Where %APPDATA% is the user application data directory, and %SID% is the textual SID of the user. However SYSTEM Master Key may be located at the following folder: %WINDIR%\System32\Microsoft\Protect.
Select Master Key file
Master Key file
9711-1363829938-1291733684-1001\1.20dfa1c6-d232-40cd-89ec-5678b380920b



hgame{EOTYNvv&Hxf!ZoCKCY!K14hK1kQ*cgP4}

真的全靠misc签到苟活了.....