Exp4-1 MD5散列值碰撞

环境设置

本实验的环境设置为Windows 11

关键步骤

1. 从书中的网址下载可执行文件 `fastcoll_v1.0.0.5.exe`
2. 运行指令 `fastcoll_v1.0.0.5.exe -p fastcoll_v1.0.0.5.exe -o m1.exe m2.exe` ，得到两个输出文件 `m1.exe` 和 `m2.exe`
3. 运行指令 `certutil -hashfile m1.exe MD5` 和 `certutil -hashfile m2.exe MD5` 得到如下两个输出：

   ```
   MD5 的 m1.exe 哈希:
   7c92d2a5cb429f820e8fde3e708ffe96
   CertUtil: -hashfile 命令成功完成。

   MD5 的 m2.exe 哈希:
   7c92d2a5cb429f820e8fde3e708ffe96
   CertUtil: -hashfile 命令成功完成。
   ```

   可以发现两个文件的MD5值是相同的。
4. 运行指令 `certutil -hashfile m1.exe SHA1` 和 `certutil -hashfile m2.exe SHA1` ，可以得到如下两个输出：

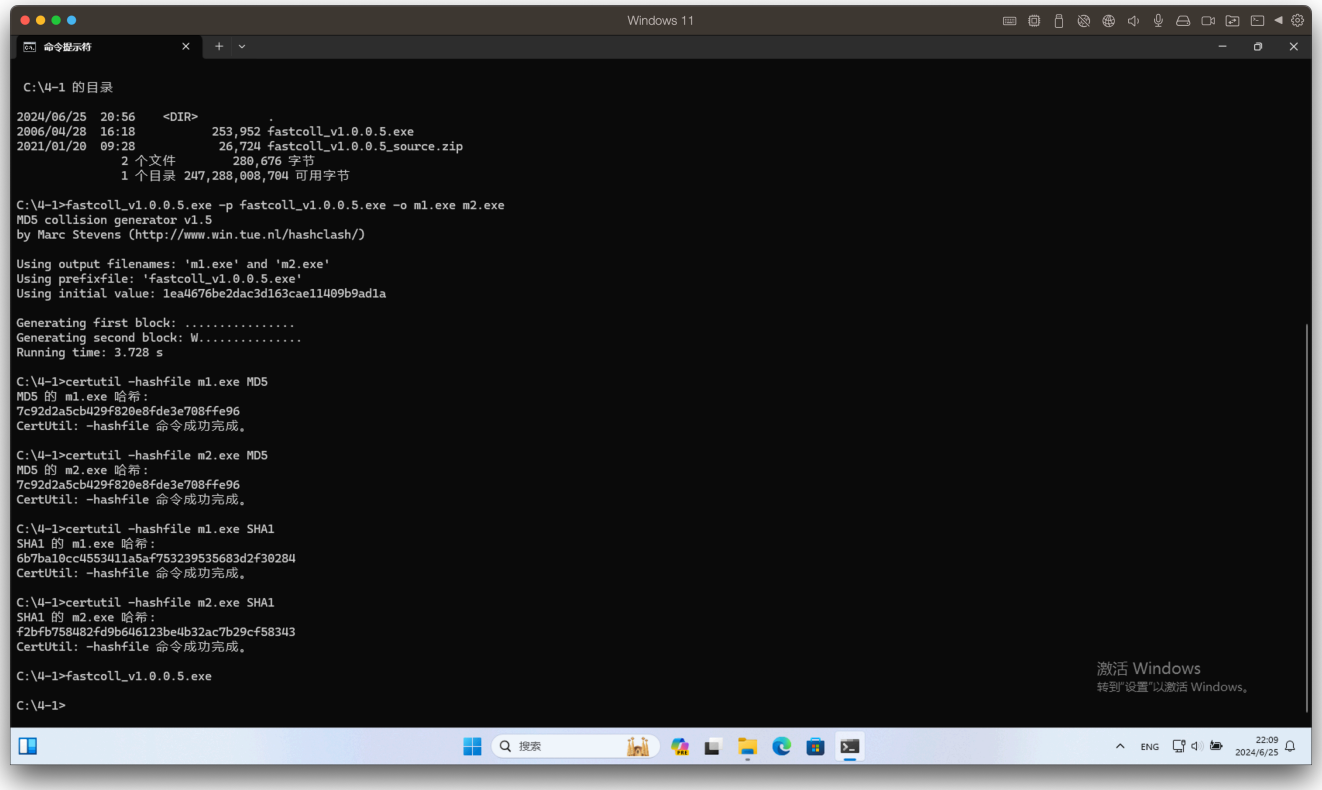
   ```
   SHA1 的 m1.exe 哈希:
   6b7ba10cc4553411a5af753239535683d2f30284
   CertUtil: -hashfile 命令成功完成。

   SHA1 的 m2.exe 哈希:
   f2bfb758482fd9b646123be4b32ac7b29cf58343
   CertUtil: -hashfile 命令成功完成。
   ```

   可以发现这两个文件的SHA1值还是不同的。

影响因素分析

不同的Hash值需要不同的碰撞方法。

实验现象


Windows 11
命令提示符
C:\4-1 的目录
2024/06/25 20:56 <DIR> .
2006/04/28 16:18 253,952 fastcoll_v1.0.0.5.exe
2021/01/20 09:28 26,724 fastcoll_v1.0.0.5_source.zip
2 个文件 280,676 字节
1 个目录 247,288,008,704 可用字节
C:\4-1>fastcoll_v1.0.0.5.exe -p fastcoll_v1.0.0.5.exe -o m1.exe m2.exe
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)
Using output filenames: 'm1.exe' and 'm2.exe'
Using prefixfile: 'fastcoll_v1.0.0.5.exe'
Using initial value: 1ea4676be2dac3d163cae11409b9ad1a
Generating first block: .....
Generating second block: W.....
Running time: 3.728 s
C:\4-1>certutil -hashfile m1.exe MD5
MD5 的 m1.exe 哈希:
7c92d2a5cb429f820e8fde3e708ffe96
CertUtil: -hashfile 命令成功完成。
C:\4-1>certutil -hashfile m2.exe MD5
MD5 的 m2.exe 哈希:
7c92d2a5cb429f820e8fde3e708ffe96
CertUtil: -hashfile 命令成功完成。
C:\4-1>certutil -hashfile m1.exe SHA1
SHA1 的 m1.exe 哈希:
6b7ba10cc4553411a5af753239535683d2f30284
CertUtil: -hashfile 命令成功完成。
C:\4-1>certutil -hashfile m2.exe SHA1
SHA1 的 m2.exe 哈希:
f2bfb758482fd9b646123be4b32ac7b29cf58343
CertUtil: -hashfile 命令成功完成。
C:\4-1>fastcoll_v1.0.0.5.exe
C:\4-1>
激活 Windows
转到"设置"以激活 Windows。
搜索
ENG
22:09
2024/6/25

关键源代码

无