

ctf练习之wireshark

原创

黎明的影 于 2020-07-22 10:42:44 发布 1517 收藏 4

分类专栏: [ctf](#) 文章标签: [安全](#)

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/SDM_JH/article/details/107507053

版权



[ctf 专栏收录该内容](#)

15 篇文章 1 订阅

订阅专栏

1.用wireshark打开题目所给的pcap文件, 在19号SMB数据包中发现password, 在16号数据包中发现Encryption Key.

```
Reserved: 00
AndxOffset: 292
Max Buffer: 4356
Max Mpx Count: 2
VC Number: 0
Session Key: 0x00000000
ANSI Password Length: 24
Unicode Password Length: 24
Reserved: 00000000
Capabilities: 0x000000d4
Byte Count (BCC): 231
ANSI Password: 9e94258a03356914b15929fa1d2e290fab9c8f9f01999448
Unicode Password: 013f3cb06ba848f98a6ae6cb4a76477c5ba4e45cda73b475
Account: syclover
Primary Domain: ROOT-53DD5427BC
Native OS: windows server 2003 3790 Service Pack 2
```

```
Word Count (wct): 17
Dialect Index: 5: NT LM 0.12
Security Mode: 0x03
Max Mpx Count: 2
Max VCs: 1
Max Buffer Size: 4356
Max Raw Buffer: 65536
Session Key: 0x00000000
Capabilities: 0x0000e3fd
System Time: Nov 15, 2014 00:08:29.000000000 [!] [!] [!] [!] [!] [!] [!]
Server Time Zone: 0 min from UTC
Key Length: 8
Byte Count (BCC): 12
Encryption Key: 1122334455667788
Primary Domain:
Server:
```

2.下载彩虹表, 使用John the Ripple工具破解密码(Linux环境)。构造一个John格式的hash文件命名为password.txt。

```
user::domain:3cf21b4522e336b068e66e034dcc1397eea57a35b9602dca:987170962556e6cafea2a2f67dc1507960f7cbc4c566143e:1122334455667788
```

它的格式为: user::domain:ANSI_Password:Unicode_Password:Encryption_Key

3.执行如下命令：`netntlm.pl --seed "NETLMIS" --file password.txt` 两次即可在john工具的目录下找到`john.pot`文件，打开即可看到密码。

```
$NETLM$1122334455667788$  
9e94258a03356914b15929fa1d  
2e290fab9c8f9f01999448:NETL  
MIS666 $NETNTLM$1122334  
455667788$013f3cb06ba848f9  
8a6ae6cb4a76477c5ba4e45cda  
73b475:NetLMis666
```