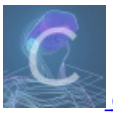
ctf练习之wireshark

原创

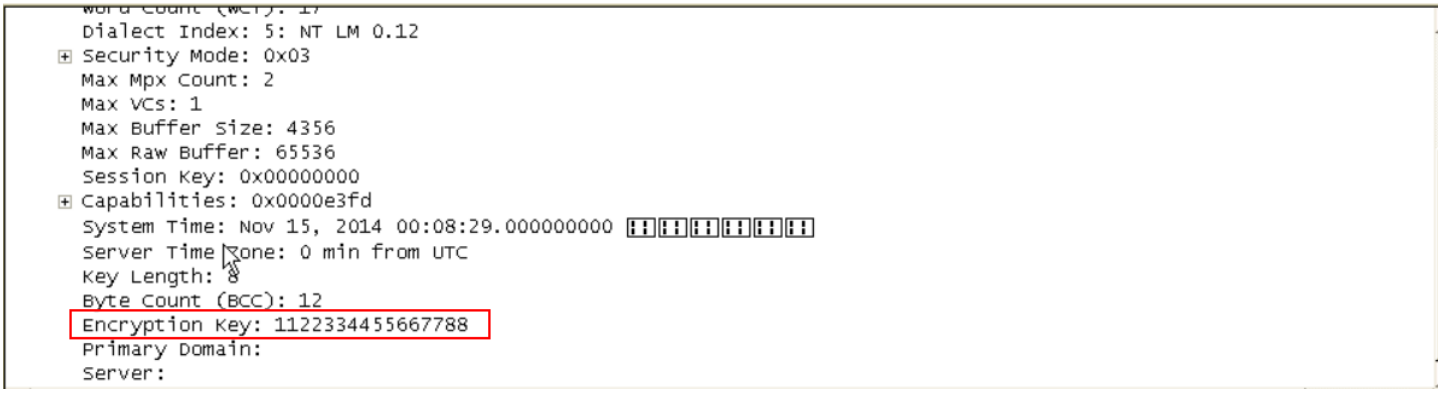
黎明的影 于 2020-07-22 10:42:44 发布 1517 收藏 4

分类专栏： ctf 文章标签： 安全

本文链接：https://blog.csdn.net/SDM_JH/article/details/107507053



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。



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:987170962556e
6cafea2a2f67dc1507960f7cbc4c566143e: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