如何使用wireshark查看SNMPV3加密报文

SNMP　夏威　2019-11-24 发表

问题描述

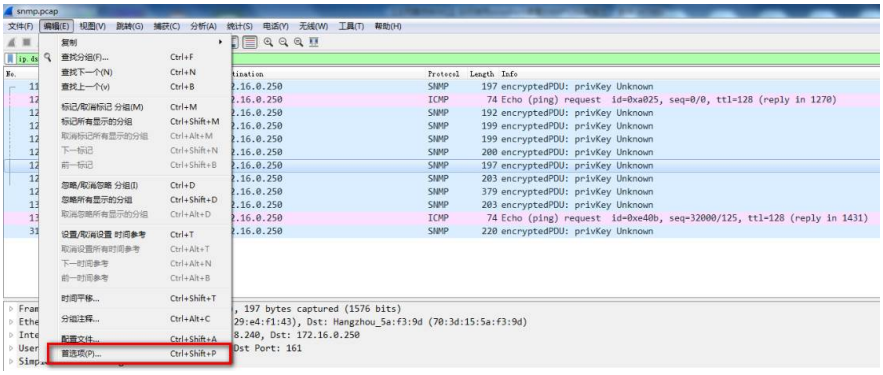
如何使用wireshark查看SNMPV3加密报文?

解决方法

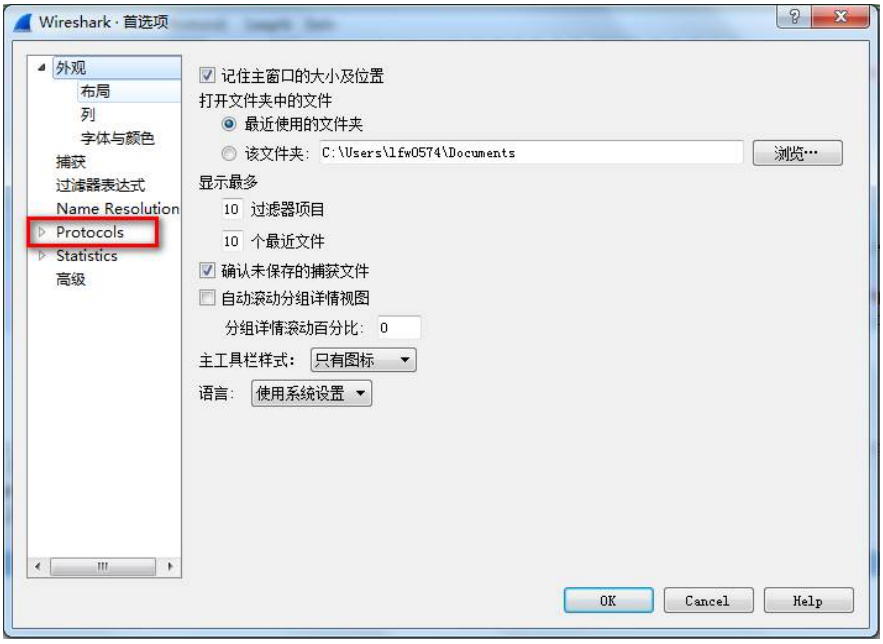
解密前的报文:

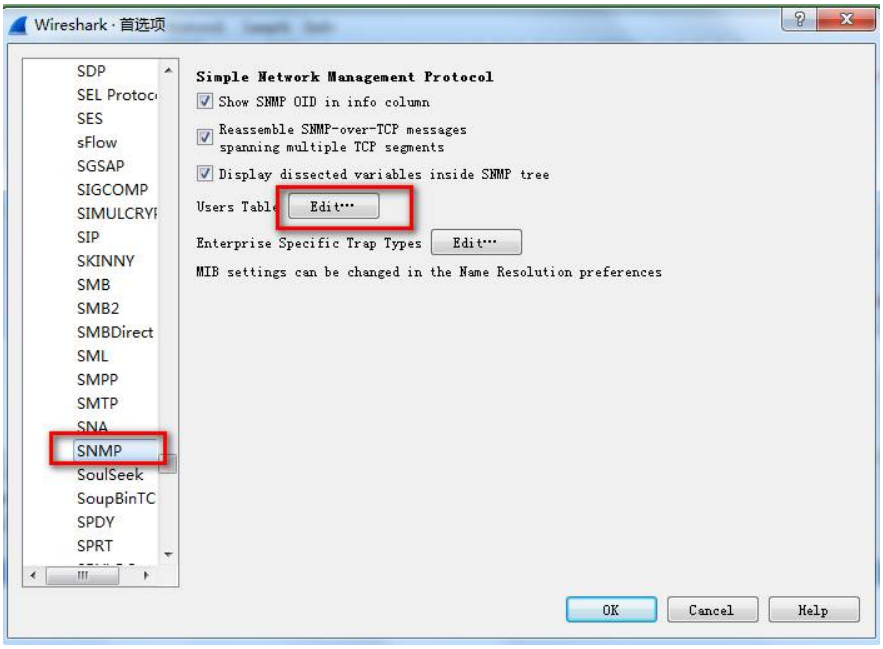
解密方法:

1、

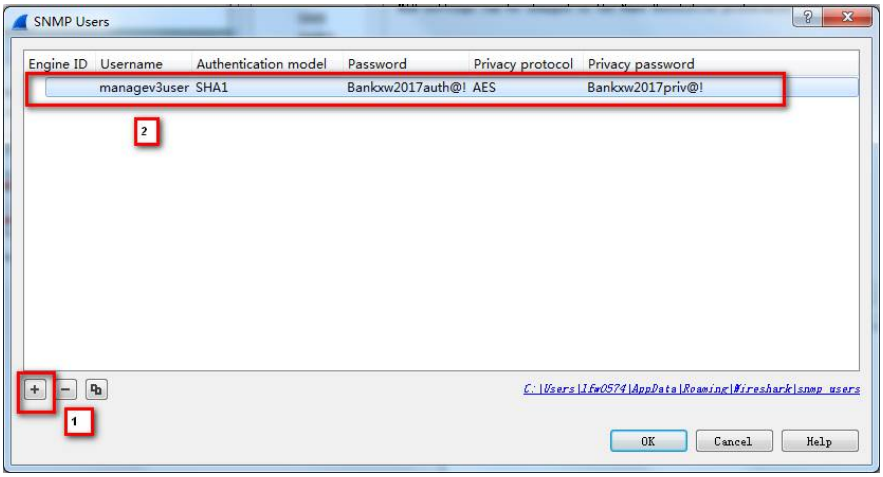


2、

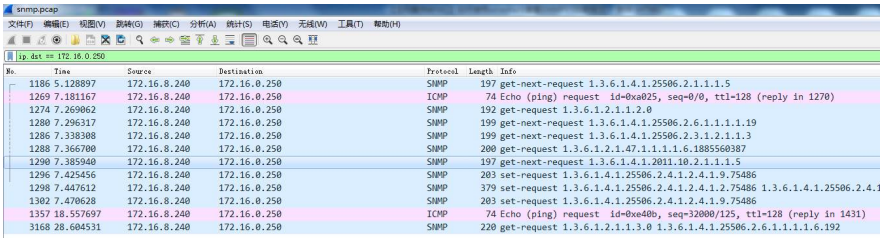



Wireshark · 首选项
SDP
SEL Protoc
SES
sFlow
SGSAP
SIGCOMP
SIMULCRYI
SIP
SKINNY
SMB
SMB2
SMBDirect
SML
SMPP
SMTP
SNA
SNMP
SoulSeek
SoupBinTC
SPDY
SPRT
Simple Network Management Protocol
Show SNMP OID in info column
Reassemble SNMP-over-TCP messages spanning multiple TCP segments
Display dissected variables inside SNMP tree
Users Table
Edit···
Enterprise Specific Trap Types
Edit···
MIB settings can be changed in the Name Resolution preferences
OK
Cancel
Help

3、


SNMP Users
Engine ID
Username
Authentication model
Password
Privacy protocol
Privacy password
managev3user
SHA1
Bankxw2017auth@!
AES
Bankxw2017priv@!
2
1
C:\Users\lfw0574\AppData\Roaming\Wireshark\snmp_users
OK
Cancel
Help

4、解密后的报文：


snmp.pcap
ip.dst == 172.16.0.250
No. Time Source Destination Protocol Length Info
1186 5.128897 172.16.8.240 172.16.0.250 SNMP 197 get-next-request 1.3.6.1.4.1.25506.2.1.1.1.5
1269 7.181167 172.16.8.240 172.16.0.250 ICMP 74 Echo (ping) request id=0xa025, seq=0/0, ttl=128 (reply in 1270)
1274 7.269062 172.16.8.240 172.16.0.250 SNMP 192 get-next-request 1.3.6.1.2.1.1.2.0
1280 7.296317 172.16.8.240 172.16.0.250 SNMP 199 get-next-request 1.3.6.1.4.1.25506.2.6.1.1.1.1.19
1286 7.338308 172.16.8.240 172.16.0.250 SNMP 199 get-next-request 1.3.6.1.4.1.25506.2.3.1.2.1.1.3
1288 7.366700 172.16.8.240 172.16.0.250 SNMP 200 get-request 1.3.6.1.2.1.47.1.1.1.1.6.1885560387
1290 7.385940 172.16.8.240 172.16.0.250 SNMP 197 get-next-request 1.3.6.1.4.1.2011.10.2.1.1.1.5
1296 7.425456 172.16.8.240 172.16.0.250 SNMP 203 set-request 1.3.6.1.4.1.25506.2.4.1.2.4.1.9.75486
1298 7.447612 172.16.8.240 172.16.0.250 SNMP 379 set-request 1.3.6.1.4.1.25506.2.4.1.2.4.1.2.75486 1.3.6.1.4.1.25506.2.4.1
1302 7.470628 172.16.8.240 172.16.0.250 SNMP 203 set-request 1.3.6.1.4.1.25506.2.4.1.2.4.1.9.75486
1357 18.557697 172.16.8.240 172.16.0.250 ICMP 74 Echo (ping) request id=0xe40b, seq=32000/125, ttl=128 (reply in 1431)
3168 28.604531 172.16.8.240 172.16.0.250 SNMP 220 get-request 1.3.6.1.2.1.1.3.0 1.3.6.1.4.1.25506.2.6.1.1.1.1.6.192