XCTF 3rd-HITB CTF-2017 arrdeepee 复现

原创

拯救の 于 2020-07-05 22:10:45 发布 703 收藏

文章标签： CTF

本文链接：https://blog.csdn.net/m0_46580995/article/details/107145246

题目说明

我们某一个box被pwn了。在检查过程中，我们发现了一个叫mimikatz的东西，我们以前没有安装过，所以我们清除了，并且重新安装了box。但是，我们忘记备份我们的flag文件了。幸运的是，我们有一个攻击者网络流量捕获。你可以帮我们恢复出flag文件吗？

得到的是一个pcap包

3757	30.247269	192.168.43.185	192.168.43.130	TLSv1	151	Application Data
3758	30.251496	192.168.43.130	192.168.43.185	UDP	43	57998 → 16384 Len=1
3759	30.261821	192.168.43.130	192.168.43.185	UDP	43	57998 → 16384 Len=1
3760	30.271662	192.168.43.130	192.168.43.185	UDP	43	57998 → 16384 Len=1
3761	30.281816	192.168.43.130	192.168.43.185	UDP	43	57998 → 16384 Len=1
3762	30.291856	192.168.43.130	192.168.43.185	TLSv1	327	Application Data
3763	30.291918	192.168.43.185	192.168.43.130	TCP	66	59921 → 3389 [ACK] Seq=48797 Ack=290677 Win=130784 Len=0 TSval=74526867 TSecr=2008311
3764	30.292150	192.168.43.130	192.168.43.185	UDP	43	57998 → 16384 Len=1
3765	30.301846	192.168.43.130	192.168.43.185	UDP	43	57998 → 16384 Len=1
3766	30.311985	192.168.43.130	192.168.43.185	UDP	43	57998 → 16384 Len=1
3767	30.322364	192.168.43.130	192.168.43.185	UDP	43	57998 → 16384 Len=1
3768	30.332186	192.168.43.130	192.168.43.185	UDP	43	57998 → 16384 Len=1
3769	30.341915	192.168.43.130	192.168.43.185	UDP	43	57998 → 16384 Len=1
3770	30.347184	192.168.43.185	192.168.43.130	TLSv1	151	Application Data

有大量的tcp和udp流

查看udp流有以下的关键字

“ TSSecKeySet1”和“ Microsoft Strong Cryptographic Provider”

```
0.      ....0.  _.      *.H..
.....   P..     L0.     H0....  *.H..
..........0...0.....*.H..
..
......0...0..
*.H..
....0...f..8]C............;G..C.\....\.5/Ho...p.?...Z^.<...+.n.#`..q}
......!...J.d..Tl.Q.........^..x............5..sx..X..]..0...&\...&.y
..J..
...R..M.{.;..|.E..q.q.?..-.:K..b.4...uI|.......9I_*...I~..e...:..&......i.(./1%S..J.[P..R.Gzm..U......2&.#<.......+
[.MSl.r.'.."...g].;..97dG.      ..z.....H.kB.}..4....Y.........h.RmH.,...^.[xnvY....)...Q.H......./...
...}......_W.m}...}.
#...:.7S....`......\..p_..b..u......'....j.....BqK.........p..=aOu.{.2....w....;r=.p........K...Eg.........x....
4...........&..9.....K..o....P.c..|...I...=^.G.|/.J.w~NR.........}..3..3P..0j...[.a.8o...A.
\4B..d..'j.G.n..b./........i*G-..k2.=..f..... ..............Z....Dt..<.T...v#._.).....
..'_.......w..Z.....M"^.(....Q...R..[.?a.t,\u%.Ll>+..Y.<..Q{..../.7..|P]+.}#.Oi...gt~.r..W.#.G...38..
..; q.....7.v...B.j6.jx...<.. .D^.l.....G#...}.U5.........{...l."z[..3..dU....@-.....j.sG%..,.q...G9..#4...gN.d.6.
..R....`...I..W.......p[.QH.;_Dh._.u...n.]z&.!...4.=\)V...D
.....'`.../...&..:98.}....$:..N.....`...Qg.0+.........B.j...j/.s"=s.kN"m?n..wSo.
....K. .6..g7a.{he./.uZ...6.Awb......,...]E.T......+B.....?...W...vf.v...%.w.O.... ....D......c|.......r...@....ZJh.u.R.M.
1...^:.8K..&..[.....hC...R)-.....
.9..C.c...@....i.       ..f.......yl.J.u.R.3-.gV.%.$';..++.:\?....Q..-k..p.1..0
.       +.....7..1.0..  *.H..
.       .1.......0'.    *.H..
.       .1....T.S.S.e.c.K.e.y.S.e.t.10].        +.....7..1P.N.M.i.c.r.o.s.o.f.t. .S.t.r.o.n.g. .C.r.y.p.t.o.g.r.a.p.h.i.c.
.P.r.o.v.i.d.e.r0..o.   *.H..
......`0..\...0..U.     *.H..
...0..
*.H..
....0....]...,.........(}.......MF....Ld../..4m.....J..+y....UZV.!..o..n.d~...)B.OU...U.........;'..9h.&4...[}4.?w.Re...
0...F.h.0....(...$#.S...;`~|...Sx...s.....q.s.Y.i.eq.>4...U....^..W.?>.`mZ...../m....z.%..@f..@[.pp...x...q..$2.O...
2.1...F.!.{].........   .l.&NX.....M.xp....J.*......z})..3..
....~|.L....6l..Z..3g   R.8.e.?...W[{.....T..Y.....<.qf.G.......09.[......z../..7...
{..........n0w...r.T.`.<.......Rs...=.........^..~../   .f)..
.{.(...w......+......[....,O.F.X.o...l.Z:7.....Lw1".d   ...JP.&pX.?f........kDC....
%<.}.#....c....O......W\.....B..i......bl......V.......}............%nO.[...\NR...Au...v?.R.*.d.'...
{H....v..n;:....Z0K?.<..JX...,4E.....&i...      ........P....5..1o...{.....<E.R..0.C...........z..o..@..gA'<L..R.d].
[......dC..../.d.s....UMd...FW.;.D..#..'.sRQw..].w.k..)...).4.3F.
G........lp
.)
....{.X....W...p...-u0:0.0...+.......ck..z@c..I......&.S.....l.....3....        j.
```


保存下来进行分析

```
user@user:~$ binwalk 1

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
30            0x1E            Certificate in DER format (x509 v3), header length: 4, sequence length: 2376
57            0x39            Certificate in DER format (x509 v3), header length: 4, sequence length: 1466
1546          0x60A           Private key in DER format (PKCS header length: 4, sequence length: 860

user@user:~$ binwalk -e 1

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
30            0x1E            Certificate in DER format (x509 v3), header length: 4, sequence length: 2376
57            0x39            Certificate in DER format (x509 v3), header length: 4, sequence length: 1466
1546          0x60A           Private key in DER format (PKCS header length: 4, sequence length: 860
```


有一些证书和私钥尝试openssl进行读取

命令：openssl asn1parse -inform DER -in

```
user@user:~$ openssl asn1parse -inform DER -in 1
    0:d=0  hl=4 l=2467 cons: SEQUENCE
    4:d=1  hl=2 l=   1 prim: INTEGER           :03
    7:d=1  hl=4 l=2399 cons: SEQUENCE
   11:d=2  hl=2 l=   9 prim: OBJECT            :pkcs7-data
   22:d=2  hl=4 l=2384 cons: cont [ 0 ]
   26:d=3  hl=4 l=2380 prim: OCTET STRING      [HEX DUMP]:308209483082 05D106092A864886F70D010701A08205C2048205BE308205BA308205B6060B2A864886F70D010C0A
0102A08204F6308204F2301C060A2A864886F70D010C0103300E040866AFD4385D4302C4020207D0048204D093F23B4782B6438E5CB094A8C35CF1352F486FA1F7E3708A3F1BFC865A5EEF
3C931DC82BA36EEF23609FE4717D0A021EEF8A981021BDADD04AFA64131A546CE65191A88C001ADCA9A5A15EDB1178E0DADDDCEDDCC3AB13BAADAE35B2B87378CC9158C0145DB1EB300E12
9D265C92E2C726E4790DA9F34AD0B80AF7BFD152B7AF4DD97B9B3BC4057CA245E4B871B871023F96832DCA3A4BA3E8628C34ACB48C75497CB8949CA48D1EF939495F2A0BE4B7497E0C1965
9EBE083ABFD8268D97149418C969CE28112F31255383994AA95B50C7A15285477A6D01B955E80C9F961FD03226C8233CA6F4851318D0B22B5B0E4D536CDF729827F2A12289E789675DDE3B
BDC339376447AF09CD807AF811D216D148126B42177D7F1634BFAB0BB959A485BE82F7CE08FA8468FE526D48B02CA70CAF5EA55B786E7659DAFEFFC8292E15C251BC48D27F15860BD32E2F
B67FB70DDED2CB7D199ECF107FEB5F57CA6D7D83ACA47DD20D23E3F7F73AF93753F1D6E6C42060A2F0A19CA9905CFCA4705F8DA96287D57584E9D0C9FEE127A1F8E91E6AA112FDD0AA4271
4BBFBDF1DB07BED4D3BB70B2AE3D614F75E17B8932E3ADCB8077DBE6EB9A3B723DFE7000B0B8DAD199D8FF4B8501BE45671BCAA8F3F5A9EB9EE67805F91C0734BE00F7EFDEAD031308879A
852612AE3910830086EF4BC3CD6F9C14C5FA50F563EAB57C89F6AA49BBDF923D5E8847017C2F134AC4777E4E52D1DDDC1CCDDF800CC07DE1E733C8D233508E88306A0C9A035B1B61FA386F
10CB1841C05C3442CAC764B0A5276A1047BF6EFA0E621A2FAE1A8792D8C5E20F692A472D88F96B32EB3D18B066BBEC04DAC120ADD3A0AFDAA2D81DF0A2CAFD1C135A0EC7AAEF4474B2853C
125487DE8A7623F25F0029F912F9F689DD0AD5F4275FC8DFB6ADD908B677D3975AFBC207B0B24D225EDF28F88C17C451D6F0A8521CA55B873F611C742C5C7525B04C6C3E2BA0BC59D43C02
EE517BA8D08E102F9837A6B37C505D2BD97D23AB4F6912B5EB67747EB572969057B923D347980E7F3338F2E70AE1E13B2071D9DD84991937B676838F8C42BB6A36A06A78B895063CBF9E20
FD445EC96CF886D58FCA47230593FE7DA25535BBDAD2BED116FCF0A47BFEE90F6C0C227A5B9DFA33BDAB645585EBD3CC402DE595FF1A016A1B73472580FB2CB271CCEDFF473916D72334E4
D5F4674EBA649636B00D05C852FFDF930360DCEFF949BEA357AF1DE79DD503E9705BAE51488F3B5F4468F15FC17593B7C06E2E5D7A26D02112E28034ED3D5C2956159CD2440D8B03BBA8E2
27608FE9C12FF0C0A12600AE3A3938AF7DDAB4BED9243A891D4EE684F5A0EC60DA908C5167F0302BBFB8940817D4C7D2F242DB6A980F196A2FF973223D73866B4E226D3F6EEB8177536FB1
0DA9E7BD864B0020C636F3A3673761A17B6865992FB0755AE9EB8036AA41776294D0FF8EA6F12CC9ECB45D45B154F2BF03B0A70E2B42DA1A7F99AA3FD4819857118FD77666D476C3C9BD25
8377994FB49EB5E820B416CCC5449895DEF2EAE3637CC8D5828D9DA7F1727FAEB740A7148BE35A4A689C75D152DD4DD431EAEA135E3AC5384BF7A226971B5BE18E041D046843F9BE855229
2DF886C97F010DE239C4DD431163A88AB440BF14BD8B69D409C48366F289E59282EDE9796CAD4A1975FF52A2332DAC6756CB25AA24273B90E22B2B133A5C3F0805160E510B192D6BC18370
F43181AC300D06092B0601040182371102310030130 6092A864886F70D010915310604040100000302706092A864886F70D010914311A1E1800540053005300650063004B006500790053
006500740031305D06092B0601040182371101310E1E004D006900630072006F0073006F006600740020005300740072006F006E006700200043007200790070007400 6F006700720061
007000680069006300200050072006F007600690064006500723082036F06092A864886F70D010706A08203603082035C020100308203550609 2A864886F70D010701301C060A2A864886
F70D010C0106300E0408135DB999CA2CD6B1020207D0808203287D8BDD108BE4C5084D46D3A88CED4C6412DF2FA7D5346D9FB289B1DC4AF4AD2B791EDA0612555A56EC21EECD6FDCCF6E83
647E8DDED72942F24F551FFCFB55B7181AE5D9B6B790EA8B3B2782013968172634810003 5B7D349B3F77FB5265FA83B73008FC1A4687687F30A3BFF0D7289BFBC82423D753F380B53B607E
7C8A101B53781D0F0273F7C1E4E42E71E2739659A569A465710B3E34C1C9165592F5DD145ECCCE570C3F3E84606D5A14878DA6172F6DB403C3FC7AF92512B8406693D4405BD27070F58A87
78C3AA8D71BDDD24327F4FC2BFD932E431B99CDD461B21B57B5D8F88E90597FDD2BCB709AF6CAA264E58C116D018DE4DEA7870B7C3BCC64A8E2A1EE29EA8CCA17A7D29B2C033E2F50ACE0E
01A87E7CF24CBCB8A9F7366C95F05ACFB233670952CA38B265CC3FC0F6D5575B7B02C50E9C0E54FDE359D0D216A80F3C817166DE479B94D81EE0FC1130392E5BBABCD6E11D807A7FEE2F95
8C3785A5857BBBFCD1B1EC8DA4D3ABFD6E3077CEB5B572C5549660B73CD3981819B2ECE1527316E5DC3DC8A0A9BFADD6A0C0065E9A8E7E1F1C2F09166629DEDC0AC57B9328C112CF77B4F3
CF0118102B94BD80B01B845B03BF079B2C4F9E461958F36FFDB7886C025A3A37D4D8E9E1804C773122FF6409FE819C4A50C1267058E93F6698DBD5D2D4D7D2EB6B4443C8D1AD0E253C1D7D
FE23E3918D1F6399EBD4CB4FC9EFE18D83DF575C06F5D21F824297E26999A4DA9FBCFB626CDDF0B2A9FDAB56CAF10785FAAD847D8589AFF8B0A39601CB1BF6B6256E4FB65BABAFFC5C4E52
08121E4175071D18763F9152962AE964DB271313D77B488C9A1AC176ADCE6E3B3A1DC092CA5A304B3FE93C1F8F4A58D8E1992C3445180FFD1EC126690E12FF09FCED1306B4D5BEB150888E
15B435AEB3316FFA019C7B89AFE0D6823C459252AF9B30E643FAC481ABE6C5E6B09C1F0B7AEEFC6FA2FC40E6BF6741273C4CFEF2529B645DFE5B7FF18AF6B9FD6443B9D206BA2F1264A073
DD1DF80E554D64DBFC934657C63BF5441CE223C1AF271C73525177ABCA5D8777916BF6D22908F3C22989349E3346BE0A4712FCF0A215B4A1F06C700A88290DA38FF6BF7B9C58DC01F0E357
02F49F70C6858E2D75
 2410:d=1  hl=2 l=  59 cons: SEQUENCE
 2412:d=2  hl=2 l=  31 cons: SEQUENCE
 2414:d=3  hl=2 l=   7 cons: SEQUENCE
 2416:d=4  hl=2 l=   5 prim: OBJECT            :sha1
 2423:d=3  hl=2 l=  20 prim: OCTET STRING      [HEX DUMP]:C6636BA1DC7A4063D2AD49F7DBB800AD92260253
 2445:d=2  hl=2 l=  20 prim: OCTET STRING      [HEX DUMP]:9BADF56CE6069E1EB9339E0E9FCD096ACD0DBC5B
 2467:d=2  hl=2 l=   2 prim: INTEGER           :07D0
```


有大量的hex，深入分析嵌套的数据，进行解码尝试

命令加一个-strparse

```
user@user:~$ openssl asn1parse -inform DER -in 1 -strparse 26
    0:d=0  hl=4 l=2376 cons: SEQUENCE
    4:d=1  hl=4 l=1489 cons: SEQUENCE
    8:d=2  hl=2 l=   9 prim: OBJECT            :pkcs7-data
   19:d=2  hl=4 l=1474 cons: cont [ 0 ]
   23:d=3  hl=4 l=1470 prim: OCTET STRING      [HEX DUMP]:308205BA308205B6060B2A864886F70D010C0A0102A08204F6308204F2301C060A2A864886F70D010C0103300E04
0866AFD4385D4302C4020207D0048204D093F23B4782B6438E5CB094A8C35CF1352F486FA1F7E3708A3F1BFC865A5EEF3C931DC82BA36EEF23609FE4717D0A021EEF8A981021BDADD04AFA
64131A546CE65191A88C001ADCA9A5A15EDB1178E0DADDDCEDDCC3AB13BAADAE35B2B87378CC9158C0145DB1EB300E129D265C92E2C726E4790DA9F34AD0B80AF7BFD152B7AF4DD97B9B3B
C4057CA245E4B871B871023F96832DCA3A4BA3E8628C34ACB48C75497CB8949CA48D1EF939495F2A0BE4B7497E0C19659EBE083ABFD8268D97149418C969CE28112F31255383994AA95B50
C7A15285477A6D01B955E80C9F961FD03226C8233CA6F4851318D0B22B5B0E4D536CDF729827F2A12289E789675DDE3BBDC339376447AF09CD807AF811D216D148126B42177D7F1634BFAB
0BB959A485BE82F7CE08FA8468FE526D48B02CA70CAF5EA55B786E7659DAFEFFC8292E15C251BC48D27F15860BD32E2FB67FB70DDED2CB7D199ECF107FEB5F57CA6D7D83ACA47DD20D23E3
F7F73AF93753F1D6E6C42060A2F0A19CA9905CFCA4705F8DA96287D57584E9D0C9FEE127A1F8E91E6AA112FDD0AA42714BBFBDF1DB07BED4D3BB70B2AE3D614F75E17B8932E3ADCB8077DB
E6EB9A3B723DFE7000B0B8DAD199D8FF4B8501BE45671BCAA8F3F5A9EB9EE67805F91C0734BE00F7EFDEAD031308879A852612AE3910830086EF4BC3CD6F9C14C5FA50F563EAB57C89F6AA
49BBDF923D5E8847017C2F134AC4777E4E52D1DDDC1CCDDF800CC07DE1E733C8D233508E88306A0C9A035B1B61FA386F10CB1841C05C3442CAC764B0A5276A1047BF6EFA0E621A2FAE1A87
92D8C5E20F692A472D88F96B32EB3D18B066BBEC04DAC120ADD3A0AFDAA2D81DF0A2CAFD1C135A0EC7AAEF4474B2853C125487DE8A7623F25F0029F912F9F689DD0AD5F4275FC8DFB6ADD9
08B677D3975AFBC207B0B24D225EDF28F88C17C451D6F0A8521CA55B873F611C742C5C7525B04C6C3E2BA0BC59D43C02EE517BA8D08E102F9837A6B37C505D2BD97D23AB4F6912B5EB6774
7EB572969057B923D347980E7F3338F2E70AE1E13B2071D9DD84991937B676838F8C42BB6A36A06A78B895063CBF9E20FD445EC96CF886D58FCA47230593FE7DA25535BBDAD2BED116FCF0
A47BFEE90F6C0C227A5B9DFA33BDAB645585EBD3CC402DE595FF1A016A1B73472580FB2CB271CCEDFF473916D72334E4D5F4674EBA649636B00D05C852FFDF930360DCEFF949BEA357AF1D
E79DD503E9705BAE51488F3B5F4468F15FC17593B7C06E2E5D7A26D02112E28034ED3D5C2956159CD2440D8B03BBA8E227608FE9C12FF0C0A12600AE3A3938AF7DDAB4BED9243A891D4EE6
84F5A0EC60DA908C5167F0302BBFB8940817D4C7D2F242DB6A980F196A2FF973223D73866B4E226D3F6EEB8177536FB10DA9E7BD864B0020C636F3A3673761A17B6865992FB0755AE9EB80
36AA41776294D0FF8EA6F12CC9ECB45D45B154F2BF03B0A70E2B42DA1A7F99AA3FD4819857118FD77666D476C3C9BD258377994FB49EB5E820B416CCC5449895DEF2EAE3637CC8D5828D9D
A7F1727FAEB740A7148BE35A4A689C75D152DD4DD431EAEA135E3AC5384BF7A226971B5BE18E041D046843F9BE8552292DF886C97F010DE239C4DD431163A88AB440BF14BD8B69D409C483
66F289E59282EDE9796CAD4A1975FF52A2332DAC6756CB25AA24273B90E22B2B133A5C3F0805160E510B192D6BC18370F43181AC300D06092B0601040182371102310030130 6092A864886
F70D010915310604040100000302706092A864886F70D010914311A1E1800540053005306500630040B0065007900530065007400313050D06092B0601040182371101315 01E4E004D0069
00630072006F0073006F006600740020005300740072006F006E006700200043007200790070007400 6F006700720061007000680069006300200050072006F007600690064006500 72
 1497:d=1  hl=4 l= 879 cons: SEQUENCE
 1501:d=2  hl=2 l=   9 prim: OBJECT            :pkcs7-encryptedData
 1512:d=2  hl=4 l= 864 cons: cont [ 0 ]
 1516:d=3  hl=4 l= 860 cons: SEQUENCE
 1520:d=4  hl=2 l=   1 prim: INTEGER           :00
 1523:d=4  hl=4 l= 853 cons: SEQUENCE
 1527:d=5  hl=2 l=   9 prim: OBJECT            :pkcs7-data
 1538:d=5  hl=2 l=  28 cons: SEQUENCE
 1540:d=6  hl=2 l=  10 prim: OBJECT            :pbeWithSHA1And40BitRC2-CBC
 1552:d=6  hl=2 l=  14 cons: SEQUENCE
 1554:d=7  hl=2 l=   8 prim: OCTET STRING      [HEX DUMP]:135DB999CA2CD6B1
 1564:d=7  hl=2 l=   2 prim: INTEGER           :07D0
 1568:d=5  hl=4 l= 808 prim: cont [ 0 ]
```


继续解码

```
user@user:~$ openssl asn1parse -inform DER -in 1 -strparse 26 -strparse 23
    0:d=0  hl=4 l=1466 cons: SEQUENCE
    4:d=1  hl=4 l=1462 cons: SEQUENCE
    8:d=2  hl=2 l=  11 prim: OBJECT            :pkcs8ShroudedKeyBag
   21:d=2  hl=4 l=1270 cons: cont [ 0 ]
   25:d=3  hl=4 l=1266 cons: SEQUENCE
   29:d=4  hl=2 l=  28 cons: SEQUENCE
```

```
   43:d=5  hl=2 l=  14 cons: SEQUENCE
   45:d=6  hl=2 l=   8 prim: OCTET STRING      [HEX DUMP]:66AFD4385D4302C4
   55:d=6  hl=2 l=   2 prim: INTEGER           :07D0
   59:d=4  hl=4 l=1232 prim: OCTET STRING      [HEX DUMP]:93F23B4782B6438E5CB094A8C35CF1352F486FA1F7E3708A3F1BFC865A5EEF3C931DC82BA36EEF23609FE4717D0A
021EEF8A981021BDADD04AFA64131A546CE65191A88C001ADCA9A5A15EDB1178E0DADDDCEDDCC3AB13BAADAE35B2B87378CC9158C0145DB1EB300E129D265C92E2C726E4790DA9F34AD0B8
0AF7BFD152B7AF4DD97B9B3BC4057CA245E4B871B871023F96832DCA3A4BA3E8628C34ACB48C75497CB8949CA48D1EF939495F2A0BE4B7497E0C19659EBE083ABFD8268D97149418C969CE
28112F31255383994AA95B50C7A15285477A6D01B955E80C9F961FD03226C8233CA6F4851318D0B22B5B0E4D536CDF729827F2A12289E789675DDE3BBDC339376447AF09CD807AF811D216
D148126B42177D7F1634BFAB0BB959A485BE82F7CE08FA8468FE526D48B02CA70CAF5EA55B786E7659DAFEFFC8292E15C251BC48D27F15860BD32E2FB67FB70DDED2CB7D199ECF107FEB5F
57CA6D7D83ACA47DD20D23E3F7F73AF93753F1D6E6C42060A2F0A19CA9905CFCA4705F8DA96287D57584E9D0C9FEE127A1F8E91E6AA112FDD0AA42714BBFBDF1DB07BED4D3BB70B2AE3D61
4F75E17B8932E3ADCB8077DBE6EB9A3B723DFE7000B0B8DAD199D8FF4B8501BE45671BCAA8F3F5A9EB9EE67805F91C0734BE00F7EFDEAD031308879A852612AE3910830086EF4BC3CD6F9C
14C5FA50F563EAB57C89F6AA49BBDF923D5E8847017C2F134AC4777E4E52D1DDDC1CCDDF800CC07DE1E733C8D233508E88306A0C9A035B1B61FA386F10CB1841C05C3442CAC764B0A5276A
1047BF6EFA0E621A2FAE1A8792D8C5E20F692A472D88F96B32EB3D18B066BBEC04DAC120ADD3A0AFDAA2D81DF0A2CAFD1C135A0EC7AAEF4474B2853C125487DE8A7623F25F0029F912F9F6
89DD0AD5F4275FC8DFB6ADD908B677D3975AFBC207B0B24D225EDF28F88C17C451D6F0A8521CA55B873F611C742C5C7525B04C6C3E2BA0BC59D43C02EE517BA8D08E102F9837A6B37C505D
2BD97D23AB4F6912B5EB67747EB572969057B923D347980E7F3338F2E70AE1E13B2071D9DD84991937B676838F8C42BB6A36A06A78B895063CBF9E20FD445EC96CF886D58FCA47230593FE
7DA25535BBDAD2BED116FCF0A47BFEE90F6C0C227A5B9DFA33BDAB645585EBD3CC402DE595FF1A016A1B73472580FB2CB271CCEDFF473916D72334E4D5F4674EBA649636B00D05C852FFDF
930360DCEFF949BEA357AF1DE79DD503E9705BAE51488F3B5F4468F15FC17593B7C06E2E5D7A26D02112E28034ED3D5C2956159CD2440D8B03BBA8E227608FE9C12FF0C0A12600AE3A3938
AF7DDAB4BED9243A891D4EE684F5A0EC60DA908C5167F0302BBFB8940817D4C7D2F242DB6A980F196A2FF973223D73866B4E226D3F6EEB8177536FB10DA9E7BD864B0020C636F3A3673761
A17B6865992FB0755AE9EB8036AA1776294D0FF8EA6F12CC9ECB45D45B154F2BF03B0A70E2B42DA1A7F99AA3FD4819857118FD77666D476C3C9BD258377994FB49EB5E820B416CCC54498
95DEF2EAE3637CC8D5828D9DA7F1727FAEB740A7148BE35A4A689C75D152DD4DD431EAEA135E3AC5384BF7A226971B5BE18E041D046843F9BE8552292DF886C97F010DE239C4DD431163A8
8AB440BF14BD8B69D409C48366F289E59282EDE9796CAD4A1975FF52A2332DAC6756CB25AA24273B90E22B2B133A5C3F0805160E510B192D6BC18370F4
 1295:d=2  hl=3 l= 172 cons: SET
 1298:d=3  hl=2 l=  13 cons: SEQUENCE
 1300:d=4  hl=2 l=   9 prim: OBJECT            :Microsoft Local Key set
 1311:d=4  hl=2 l=   0 cons: SET
 1313:d=3  hl=2 l=  19 cons: SEQUENCE
 1315:d=4  hl=2 l=   9 prim: OBJECT            :localKeyID
 1326:d=4  hl=2 l=   6 cons: SET
 1328:d=5  hl=2 l=   4 prim: OCTET STRING      [HEX DUMP]:01000000
 1334:d=3  hl=2 l=  39 cons: SEQUENCE
 1336:d=4  hl=2 l=   9 prim: OBJECT            :friendlyName
 1347:d=4  hl=2 l=  26 cons: SET
 1349:d=5  hl=2 l=  24 prim: BMPSTRING
 1375:d=3  hl=2 l=  93 cons: SEQUENCE
 1377:d=4  hl=2 l=   9 prim: OBJECT            :Microsoft CSP Name
 1388:d=4  hl=2 l=  80 cons: SET
 1390:d=5  hl=2 l=  78 prim: BMPSTRING
```


有可能是密钥

```
user@user:~$ openssl asn1parse -inform DER -in 1 -strparse 26 -strparse 23
    0:d=0  hl=4 l=1466 cons: SEQUENCE
    4:d=1  hl=4 l=1462 cons: SEQUENCE
    8:d=2  hl=2 l=  11 prim: OBJECT            :pkcs8ShroudedKeyBag
   21:d=2  hl=4 l=1270 cons: cont [ 0 ]
   25:d=3  hl=4 l=1266 cons: SEQUENCE
   29:d=4  hl=2 l=  28 cons: SEQUENCE
   31:d=5  hl=2 l=  10 prim: OBJECT            :pbeWithSHA1And3-KeyTripleDES-CBC
   43:d=5  hl=2 l=  14 cons: SEQUENCE
   45:d=6  hl=2 l=   8 prim: OCTET STRING      [HEX DUMP]:66AFD4385D4302C4
   55:d=6  hl=2 l=   2 prim: INTEGER           :07D0
   59:d=4  hl=4 l=1232 prim: OCTET STRING      [HEX DUMP]:93F23B4782B6438E5CB094A8C35CF1352F486FA1F7E3708A3F1BFC865A5EEF3C931DC82BA36EEF23609FE4717D0A
021EEF8A981021BDADD04AFA64131A546CE65191A88C001ADCA9A5A15EDB1178E0DADDDCEDDCC3AB13BAADAE35B2B87378CC9158C0145DB1EB300E129D265C92E2C726E4790DA9F34AD0B8
0AF7BFD152B7AF4DD97B9B3BC4057CA245E4B871B871023F96832DCA3A4BA3E8628C34ACB48C75497CB8949CA48D1EF939495F2A0BE4B7497E0C19659EBE083ABFD8268D97149418C969CE
28112F31255383994AA95B50C7A15285477A6D01B955E80C9F961FD03226C8233CA6F4851318D0B22B5B0E4D536CDF729827F2A12289E789675DDE3BBDC339376447AF09CD807AF811D216
D148126B42177D7F1634BFAB0BB959A485BE82F7CE08FA8468FE526D48B02CA70CAF5EA55B786E7659DAFEFFC8292E15C251BC48D27F15860BD32E2FB67FB70DDED2CB7D199ECF107FEB5F
57CA6D7D83ACA47DD20D23E3F7F73AF93753F1D6E6C42060A2F0A19CA9905CFCA4705F8DA96287D57584E9D0C9FEE127A1F8E91E6AA112FDD0AA42714BBFBDF1DB07BED4D3BB70B2AE3D61
4F75E17B8932E3ADCB8077DBE6EB9A3B723DFE7000B0B8DAD199D8FF4B8501BE45671BCAA8F3F5A9EB9EE67805F91C0734BE00F7EFDEAD031308879A852612AE3910830086EF4BC3CD6F9C
14C5FA50F563EAB57C89F6AA49BBDF923D5E8847017C2F134AC4777E4E52D1DDDC1CCDDF800CC07DE1E733C8D233508E88306A0C9A035B1B61FA386F10CB1841C05C3442CAC764B0A5276A
1047BF6EFA0E621A2FAE1A8792D8C5E20F692A472D88F96B32EB3D18B066BBEC04DAC120ADD3A0AFDAA2D81DF0A2CAFD1C135A0EC7AAEF4474B2853C125487DE8A7623F25F0029F912F9F6
89DD0AD5F4275FC8DFB6ADD908B677D3975AFBC207B0B24D225EDF28F88C17C451D6F0A8521CA55B873F611C742C5C7525B04C6C3E2BA0BC59D43C02EE517BA8D08E102F9837A6B37C505D
2BD97D23AB4F6912B5EB67747EB572969057B923D347980E7F3338F2E70AE1E13B2071D9DD84991937B676838F8C42BB6A36A06A78B895063CBF9E20FD445EC96CF886D58FCA47230593FE
7DA25535BBDAD2BED116FCF0A47BFEE90F6C0C227A5B9DFA33BDAB645585EBD3CC402DE595FF1A016A1B73472580FB2CB271CCEDFF473916D72334E4D5F4674EBA649636B00D05C852FFDF
930360DCEFF949BEA357AF1DE79DD503E9705BAE51488F3B5F4468F15FC17593B7C06E2E5D7A26D02112E28034ED3D5C2956159CD2440D8B03BBA8E227608FE9C12FF0C0A12600AE3A3938
AF7DDAB4BED9243A891D4EE684F5A0EC60DA908C5167F0302BBFB8940817D4C7D2F242DB6A980F196A2FF973223D73866B4E226D3F6EEB8177536FB10DA9E7BD864B0020C636F3A3673761
A17B6865992FB0755AE9EB8036AA1776294D0FF8EA6F12CC9ECB45D45B154F2BF03B0A70E2B42DA1A7F99AA3FD4819857118FD77666D476C3C9BD258377994FB49EB5E820B416CCC54498
95DEF2EAE3637CC8D5828D9DA7F1727FAEB740A7148BE35A4A689C75D152DD4DD431EAEA135E3AC5384BF7A226971B5BE18E041D046843F9BE8552292DF886C97F010DE239C4DD431163A8
8AB440BF14BD8B69D409C48366F289E59282EDE9796CAD4A1975FF52A2332DAC6756CB25AA24273B90E22B2B133A5C3F0805160E510B192D6BC18370F4
 1295:d=2  hl=3 l= 172 cons: SET
 1298:d=3  hl=2 l=  13 cons: SEQUENCE
 1300:d=4  hl=2 l=   9 prim: OBJECT            :Microsoft Local Key set
 1311:d=4  hl=2 l=   0 cons: SET
 1313:d=3  hl=2 l=  19 cons: SEQUENCE
 1315:d=4  hl=2 l=   9 prim: OBJECT            :localKeyID
 1326:d=4  hl=2 l=   6 cons: SET
 1328:d=5  hl=2 l=   4 prim: OCTET STRING      [HEX DUMP]:01000000
 1334:d=3  hl=2 l=  39 cons: SEQUENCE
 1336:d=4  hl=2 l=   9 prim: OBJECT            :friendlyName
 1347:d=4  hl=2 l=  26 cons: SET
 1349:d=5  hl=2 l=  24 prim: BMPSTRING
 1375:d=3  hl=2 l=  93 cons: SEQUENCE
 1377:d=4  hl=2 l=   9 prim: OBJECT            :Microsoft CSP Name
 1388:d=4  hl=2 l=  80 cons: SET
 1390:d=5  hl=2 l=  78 prim: BMPSTRING
user@user:~$ openssl pkcs12 -in 1 -nocerts -nodes -out private.key
```


提取出来

```
user@user:~$ openssl pkcs12 -in 1 -nocerts -nodes -out private.key
Enter Import Password:
Mac verify error: invalid password?
```

提取需要密码结合题目的 mimikatz（https://github.com/FreeRDP/FreeRDP/wiki/Mimikatz）尝试做密码

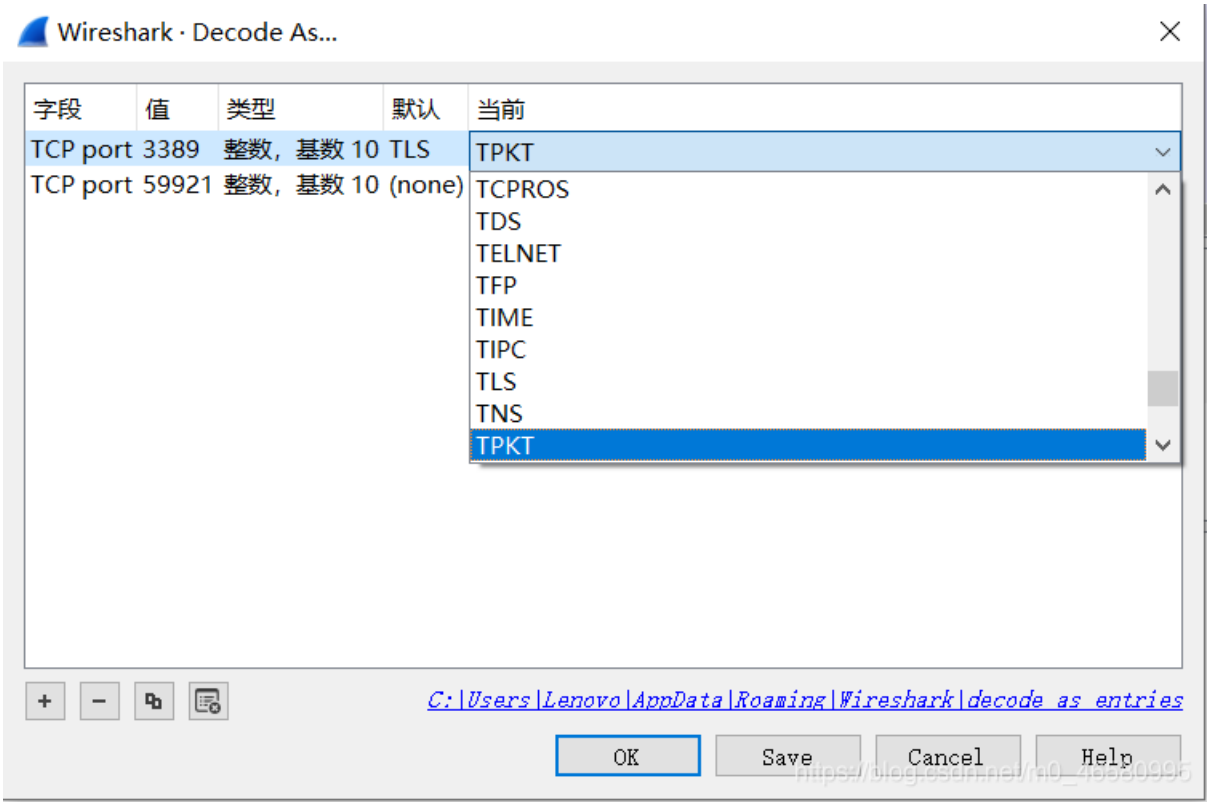
```
user@user:~$ openssl pkcs12 -in 1 -nocerts -nodes -out private.key
Enter Import Password:
```

成功提取

回过头看pcap包

1	0.000000	192.168.43.185	192.168.43.130	TCP	78 59921 → 3389 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=74497007 TSecr=0 SACK
2	0.000348	192.168.43.130	192.168.43.185	TCP	74 3389 → 59921 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=2005281
3	0.000384	192.168.43.185	192.168.43.130	TCP	66 59921 → 3389 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=74497007 TSecr=2005281
4	0.000440	192.168.43.185	192.168.43.130	RDP	110 Cookie: mstshash=IEUser, Negotiate Request
5	0.003755	192.168.43.130	192.168.43.185	TCP	66 3389 → 59921 [ACK] Seq=1 Ack=45 Win=66560 Len=0 TSval=2005282 TSecr=74497007
6	0.003908	192.168.43.130	192.168.43.185	RDP	85 Negotiate Response
7	0.003943	192.168.43.185	192.168.43.130	TCP	66 59921 → 3389 [ACK] Seq=45 Ack=20 Win=131744 Len=0 TSval=74497010 TSecr=2005282
8	0.012047	192.168.43.185	192.168.43.130	TPKT	133 Continuation
9	0.012439	192.168.43.130	192.168.43.185	TPKT	894 Continuation
10	0.012479	192.168.43.185	192.168.43.130	TCP	66 59921 → 3389 [ACK] Seq=112 Ack=848 Win=130912 Len=0 TSval=74497018 TSecr=2005283
11	0.013853	192.168.43.185	192.168.43.130	TPKT	392 Continuation
12	0.018763	192.168.43.130	192.168.43.185	TPKT	125 Continuation
13	0.018813	192.168.43.185	192.168.43.130	TCP	66 59921 → 3389 [ACK] Seq=438 Ack=907 Win=131008 Len=0 TSval=74497023 TSecr=2005283
14	0.019030	192.168.43.185	192.168.43.130	TPKT	551 Continuation
15	0.019522	192.168.43.130	192.168.43.185	TPKT	215 Continuation
16	0.019562	192.168.43.185	192.168.43.130	TCP	66 59921 → 3389 [ACK] Seq=923 Ack=1056 Win=130912 Len=0 TSval=74497023 TSecr=2005283
17	0.019615	192.168.43.185	192.168.43.130	TPKT	119 Continuation
18	0.019629	192.168.43.185	192.168.43.130	TPKT	103 Continuation
19	0.019800	192.168.43.130	192.168.43.185	TCP	66 3389 → 59921 [ACK] Seq=1056 Ack=1013 Win=65536 Len=0 TSval=2005283 TSecr=74497023

有RDP和TPKT包（如果没有就右键decode解码）



其中的RDP 可以通过rdp_replay来重播RDP会话

命令

replay/rdp_replay -r 1.pcap -o recording.avi -p ./private.key --save_clipboard --show_keys > output

https://download.csdn.net/download/m0_46580995/12579907

通过视频（视频等上传通过）可以知道攻击者，他的工作是使用未显示给用户的密码压缩和加密标志文件，然后将base64编码并复制到剪贴板。
上一步已经把键位和剪切板下载下来

```
root@route:/home/route/RDP-Replay# cat output
RDP SSL MODE Requested by server!!
SSL private key found.
1024x756x8
REALLY DELICIOUS PANCAKES<Tab>REALLY DELICIOUS PANCAKESroot@route:/home/route/RD
P-Replay# ls
```

```
root@route:/home/route/RDP-Replay# ls
1.pcap               libfree_rdp  output       recording.avi  tools
clip-00000000-down   LICENSE      private.key  replay
extractrdpkeys       Makefile     README       test
root@route:/home/route/RDP-Replay# cat clip-00000000-down
N3q8ryccAATjAlOVMAAAAAAAAABqAAAAAAAAACmoQ4fA1DQXZvCzJGIg/8cxnh8QXnWoDkwNxjGL
37P7rvVC2SMn8+wquEv/A5HBL9djQewBBAYAAQkwAAcLAQACJAbxBwEKUweBdxD1DDirkCEhAQAB
AAwrJwAICgGwcALcAAAFARkJAAAAAAAAAAAAERMAZgBsAGEAZwAuAHQAeAB0AAAAGQAUCgEAAFNu
lssb0wEVBgEAIAAAAAAA
```


以及粘贴板上的base64解码并写入文件发现一个7z压缩包

```
root@route:/home/route/RDP-Replay# 7z x flag.7z

7-Zip [64] 9.20  Copyright (c) 1999-2010 Igor Pavlov  2010-11-18
p7zip Version 9.20 (locale=zh_CN.UTF-8,Utf16=on,HugeFiles=on,1 CPU)

Processing archive: flag.7z


Enter password (will not be echoed) :
Extracting  flag.txt

Everything is Ok

Size:       39
Compressed: 186
```


需要密码就是键盘键入的
RDP SSL MODE Requested by server!!
SSL private key found.
1024x756x8
REALLY DELICIOUS PANCAKESREALLY DELICIOUS PANCAKES

得到flag

```
root@route:/home/route/RDP-Replay# cat flag.txt
HITB{44519a67ffc654e40febc09e20e8e745}
root@route:/home/route/RDP-Replay#
```