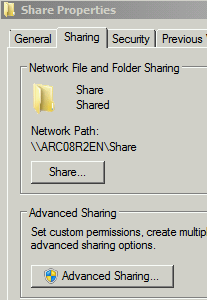
1. 示例环境

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | IP | OS | 角色 |
| ARDC08R2EN | 192.168.1.1 | Windows 2008 R2 | DC&DNS |
| ARCWin7EN | 192.168.1.14 | Windows 7 | Client |
| ARC08R2EN | 192.168.1.11 | Windows 2008 R2 | Server |

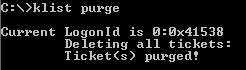
在ARCWin7EN上安装Network Monitor

<http://www.microsoft.com/en-in/download/details.aspx?id=4865>

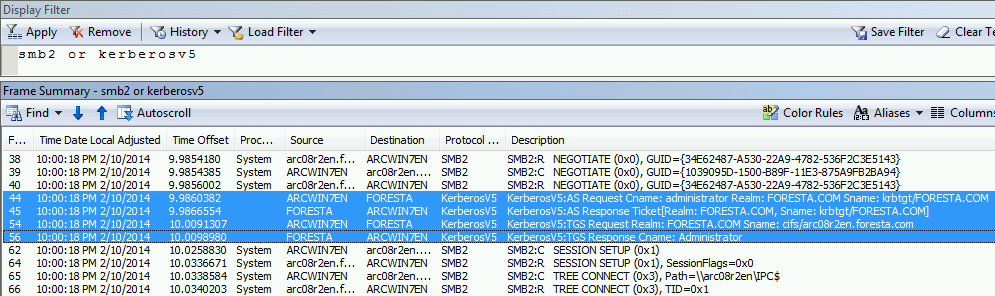
1. 抓取正常访问共享网络包，查看Kerberos验证流程
2. 在ARC08R2EN上创建共享文件夹



1. 在ARCWin7EN上用管理员权限打开命令行，运行klist purge清空票据



1. 在ARCWin7EN上打开Network monitor，开始抓包
2. 打开Windows Explorer，访问[\\ARC08R2EN\Share](file:///\\\\ARC08R2EN\\Share)
3. 访问成功后，停止抓包，过滤smb2 or kerberosv5



观察高亮的每一帧，并与之前学习的消息内容进行比较：（参考M08\_Lab\_2.cap网络包）

例如，KRB\_AS\_REQ的内容如下：

Frame: Number = 44, Captured Frame Length = 365, MediaType = ETHERNET

+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-09-39-09],SourceAddress:[00-15-5D-09-39-10]

+ Ipv4: Src = 192.168.1.14, Dest = 192.168.1.1, Next Protocol = TCP, Packet ID = 2385, Total IP Length = 351

+ Tcp: Flags=...AP..., SrcPort=61352, DstPort=Kerberos(88), PayloadLen=311, Seq=3800602383 - 3800602694, Ack=2642500902, Win=513 (scale factor 0x8) = 131328

- Kerberos: AS Request Cname: administrator Realm: FORESTA.COM Sname: krbtgt/FORESTA.COM

+ Length: Length = 307

- AsReq: Kerberos AS Request

+ ApplicationTag:

- KdcReq: KRB\_AS\_REQ (10)

+ SequenceHeader:

+ Tag1:

+ Pvno: 5

+ Tag2:

+ MsgType: KRB\_AS\_REQ (10)

+ Tag3:

- PaData:

+ SequenceOfHeader:

- PaData: PA-ENC-TIMESTAMP (2)

+ SequenceHeader:

+ Tag1:

+ PaDataType: PA-ENC-TIMESTAMP (2)

+ Tag2:

+ OctetStringHeader:

- KrbEncTimestamp: Encrypted Timestamp Pre-authentication

- PaEncTsEnc:

+ SequenceHeader:

+ Tag0:

+ EType: rc4-hmac (23)

+ Tag2:

+ Cipher: Èð•M­Ó¡¦D;IkTn6¨zï”‑\*þ¯ÝMÈaüý›|(ÔÕtAÕ Ëùïñn

- PaData: PA-PAC-REQUEST (128)

+ SequenceHeader:

+ Tag1:

+ PaDataType: PA-PAC-REQUEST (128)

+ Tag2:

+ OctetStringHeader:

- PaPacRequest:

+ SequenceHeader:

+ Tag0:

+ IncludePac: True

+ Tag4:

- ReqBody:

+ SequenceHeader:

+ Tag0:

+ KdcOptions: 0x40810010

+ Tag1:

+ Cname: administrator

+ Tag2: 0x1

+ Realm: FORESTA.COM

+ Tag3:

+ Sname: krbtgt/FORESTA.COM

+ Tag5: 0x1

+ Till: 09/13/2037 02:48:05 UTC

+ Tag6:

+ Rtime: 09/13/2037 02:48:05 UTC

+ Tag7:

+ Nonce: 1878469239 (0x6FF72A77)

+ Tag8:

- Etype:

+ SequenceOfHeader:

+ EType: aes256-cts-hmac-sha1-96 (18)

+ EType: aes128-cts-hmac-sha1-96 (17)

+ EType: rc4-hmac (23)

+ EType: rc4-hmac-exp (24)

+ EType: Unknown Encryption Type (0xff79)

+ EType: des-cbc-md5 (3)

+ Tag9:

+ Addresses:

KRB\_AS\_REP的内容如下：

Frame: Number = 45, Captured Frame Length = 1514, MediaType = ETHERNET

+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-09-39-10],SourceAddress:[00-15-5D-09-39-09]

+ Ipv4: Src = 192.168.1.1, Dest = 192.168.1.14, Next Protocol = TCP, Packet ID = 20643, Total IP Length = 1500

+ Tcp: Flags=...A...., SrcPort=Kerberos(88), DstPort=61352, PayloadLen=1460, Seq=2642500902 - 2642502362, Ack=3800602694, Win=513 (scale factor 0x8) = 131328

- Kerberos: AS Response Ticket[Realm: FORESTA.COM, Sname: krbtgt/FORESTA.COM]

+ Length: Length = 1467

- AsRep: Kerberos AS Response

+ ApplicationTag:

- KdcRep: KRB\_AS\_REP (11)

+ SequenceHeader:

+ Tag0:

+ PvNo: 5

+ Tag1:

+ MsgType: KRB\_AS\_REP (11)

+ Tag3:

+ Crealm: FORESTA.COM

+ Tag4:

+ Cname: Administrator

+ Tag5:

- Ticket: Realm: FORESTA.COM, Sname: krbtgt/FORESTA.COM

+ ApplicationTag:

+ SequenceHeader:

+ Tag0:

+ TktVno: 5

+ Tag1:

+ Realm: FORESTA.COM

+ Tag2: 0x1

+ Sname: krbtgt/FORESTA.COM

+ Tag3: 0x1

- EncPart:

+ SequenceHeader:

+ Tag0:

+ EType: rc4-hmac (23)

+ Tag1:

+ KvNo: 2

+ Tag2:

+ Cipher: "—xÂ Šz‹;7‰L=QZ6œÌ«É1ds’ì`9P‘YŸ¥Qˆ˜x9ÞulœNfÂ{ö>®îõÅºo®kgH‹ñ¯LÅ®-Ð\*Kº8¦8é'Ÿ»ªÈa§£pŠø¾Åò»•xE|ÉA:êÛ¸cBôc`YF¢^~„Ètš8¸¸^ºE¤JuÅ¨™šÙ`&nl N ZJã©÷–l°zu/$ðÑ6ŸàÿšU`ŠË}\_mçÊ¢¡o,66„d2$Pð˜í™T  
·ô1›IBƒëéôÜ§F?b÷ï0¦º!»Ñr

&]òHK‹wÚá

¤Sœ¨ÿ~X¶ß

+ Tag6:

- EncPart:

+ SequenceHeader:

+ Tag0:

+ EType: rc4-hmac (23)

+ Tag1:

+ KvNo: 1

+ Tag2:

+ Cipher: òmÄØŠPÎ’Ñúxõ£jÔèýïhå”«ï>–pÚWe#g»•ËX,i¦ª…‰c^µ© x^òâ—IÔ‹ì …¼x‘0Éb;I>HÍUN³£B0©åA4×‰È"3H?º§ä#Ý°+@[ü¨‰‹£5eã]9óäðý”7¼X2/¿Ÿþ8rÝ+3Y7)aç=xÐ\*<Ð ¼â®‑DðÕÜîìlòñëÝXl×v?V& WC+²

KRB\_TGS\_REQ的内容如下：

Frame: Number = 54, Captured Frame Length = 1629, MediaType = ETHERNET

+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-09-39-09],SourceAddress:[00-15-5D-09-39-10]

+ Ipv4: Src = 192.168.1.14, Dest = 192.168.1.1, Next Protocol = TCP, Packet ID = 2390, Total IP Length = 0

+ Tcp: Flags=...AP..., SrcPort=61353, DstPort=Kerberos(88), PayloadLen=1575, Seq=2279507912 - 2279509487, Ack=2906486498, Win=513 (scale factor 0x8) = 131328

- Kerberos: TGS Request Realm: FORESTA.COM Sname: cifs/arc08r2en.foresta.com

+ Length: Length = 1571

- TgsReq: Kerberos TGS Request

+ ApplicationTag:

- KdcReq: KRB\_TGS\_REQ (12)

+ SequenceHeader:

+ Tag1:

+ Pvno: 5

+ Tag2:

+ MsgType: KRB\_TGS\_REQ (12)

+ Tag3:

- PaData:

+ SequenceOfHeader:

- PaData: PA-TGS-REQ (1)

+ SequenceHeader:

+ Tag1:

+ PaDataType: PA-TGS-REQ (1)

+ Tag2:

+ OctetStringHeader:

- KrbApReq: KRB\_AP\_REQ (14)

+ ApplicationTag:

+ SequenceHeader:

+ Tag0:

+ PvNo: 5

+ Tag1:

+ MsgType: KRB\_AP\_REQ (14)

+ Tag2: 0x1

+ ApOptions:

+ Tag3:

- Ticket: Realm: FORESTA.COM, Sname: krbtgt/FORESTA.COM

+ ApplicationTag:

+ SequenceHeader:

+ Tag0:

+ TktVno: 5

+ Tag1:

+ Realm: FORESTA.COM

+ Tag2: 0x1

+ Sname: krbtgt/FORESTA.COM

+ Tag3: 0x1

+ EncPart:

+ Tag4:

- Authenticator:

+ SequenceHeader:

+ Tag0:

+ EType: rc4-hmac (23)

+ Tag2:

+ Cipher: Æù’W‚&ƒ,!¾õ\_&ÍÒ-ÁäUA‚ë»„ÿK²Î ¸NåLœfUSMOèÍ ­r™äâ›¶èbN<‰

+ Tag4:

- ReqBody:

+ SequenceHeader:

+ Tag0:

+ KdcOptions: 0x40810000

+ Tag2: 0x1

+ Realm: FORESTA.COM

+ Tag3:

+ Sname: cifs/arc08r2en.foresta.com

+ Tag5: 0x1

+ Till: 09/13/2037 02:48:05 UTC

+ Tag7:

+ Nonce: 1878165724 (0x6FF288DC)

+ Tag8:

- Etype:

+ SequenceOfHeader:

+ EType: aes256-cts-hmac-sha1-96 (18)

+ EType: aes128-cts-hmac-sha1-96 (17)

+ EType: rc4-hmac (23)

+ EType: rc4-hmac-exp (24)

+ EType: Unknown Encryption Type (0xff79)

+ TagA:

- EncAuthorizationData:

+ SequenceHeader:

+ Tag0:

+ EType: rc4-hmac (23)

+ Tag2:

+ Cipher: Ñ¤ët'`¡þ\*QawK9ÚÞAë<±F»;Jk#"Á  
|º³ß¹ªµm]

KRB\_TGS\_REP的内容如下：

Frame: Number = 56, Captured Frame Length = 1514, MediaType = ETHERNET

+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-09-39-10],SourceAddress:[00-15-5D-09-39-09]

+ Ipv4: Src = 192.168.1.1, Dest = 192.168.1.14, Next Protocol = TCP, Packet ID = 20649, Total IP Length = 1500

+ Tcp: Flags=...A...., SrcPort=Kerberos(88), DstPort=61353, PayloadLen=1460, Seq=2906486498 - 2906487958, Ack=2279509487, Win=513 (scale factor 0x8) = 131328

- Kerberos: TGS Response Cname: Administrator

+ Length: Length = 1648

- TgsRep: Kerberos TGS Response

+ ApplicationTag:

- KdcRep: KRB\_TGS\_REP (13)

+ SequenceHeader:

+ Tag0:

+ PvNo: 5

+ Tag1:

+ MsgType: KRB\_TGS\_REP (13)

+ Tag3:

+ Crealm: FORESTA.COM

+ Tag4:

+ Cname: Administrator

+ Tag5:

- Ticket: Realm: FORESTA.COM, Sname: cifs/arc08r2en.foresta.com

+ ApplicationTag:

+ SequenceHeader:

+ Tag0:

+ TktVno: 5

+ Tag1:

+ Realm: FORESTA.COM

+ Tag2: 0x1

+ Sname: cifs/arc08r2en.foresta.com

+ Tag3: 0x1

- EncPart:

+ SequenceHeader:

+ Tag0:

+ EType: aes256-cts-hmac-sha1-96 (18)

+ Tag1:

+ KvNo: 1

+ Tag2:

+ Cipher: óÜˆ?wsN7ÐJ'ÅZ”öë÷HHƒ«NM~‚\§Rß¹

+ Tag6:

- EncPart:

+ SequenceHeader:

+ Tag0:

+ EType: rc4-hmac (23)

+ Tag2:

+ Cipher: õþ¤j²õ\*¾ÿ¨Be–ÊÆPëØ[h¿LDˆ‡)òEÅ=Xq¥ ªYS±É¤«‚³Šìê8‡£Â¢àèâ×8ÞiÁ6©O‰Ó®¯·Óµ}Ödû

KRB\_AP\_REQ被包含在了SMB的网络包中，内容如下：

Frame: Number = 62, Captured Frame Length = 1906, MediaType = ETHERNET

+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-09-39-0B],SourceAddress:[00-15-5D-09-39-10]

+ Ipv4: Src = 192.168.1.14, Dest = 192.168.1.11, Next Protocol = TCP, Packet ID = 2394, Total IP Length = 0

+ Tcp: Flags=...AP..., SrcPort=61351, DstPort=Microsoft-DS(445), PayloadLen=1852, Seq=2185086111 - 2185087963, Ack=2603305888, Win=511 (scale factor 0x8) = 130816

+ SMBOverTCP: Length = 1848

- SMB2: C SESSION SETUP (0x1)

SMBIdentifier: SMB

+ SMB2Header: C SESSION SETUP (0x1),TID=0x0000, MID=0x0002, PID=0xFEFF, SID=0x0000

- CSessionSetup:

StructureSize: 25 (0x19)

VcNumber: 0 (0x0)

+ SecurityMode: 1 (0x1)

+ Capabilities: 0x1

Channel: 0 (0x0)

SecurityBufferOffset: 88 (0x58)

SecurityBufferLength: 1760 (0x6E0)

PreviousSessionId: 0 (0x0)

- securityBlob:

- GSSAPI:

- InitialContextToken:

+ ApplicationHeader:

+ ThisMech: SpnegoToken (1.3.6.1.5.5.2)

- InnerContextToken: 0x1

- SpnegoToken: 0x1

+ ChoiceTag:

- NegTokenInit:

+ SequenceHeader:

+ Tag0:

+ MechTypes: Prefer MsKerberosToken (1.2.840.48018.1.2.2)

+ Tag2:

+ OctetStringHeader:

- MechToken: 0x1

- MsKerberosToken: 0x1

- KerberosInitToken:

+ ApplicationHeader:

+ ThisMech: KerberosToken (1.2.840.113554.1.2.2)

- InnerContextToken: 0x1

- KerberosToken: 0x1

TokId: Krb5ApReq (0x100)

- ApReq: KRB\_AP\_REQ (14)

+ ApplicationTag:

+ SequenceHeader:

+ Tag0:

+ PvNo: 5

+ Tag1:

+ MsgType: KRB\_AP\_REQ (14)

+ Tag2: 0x1

+ ApOptions:

+ Tag3:

- Ticket: Realm: FORESTA.COM, Sname: cifs/arc08r2en.foresta.com

+ ApplicationTag:

+ SequenceHeader:

+ Tag0:

+ TktVno: 5

+ Tag1:

+ Realm: FORESTA.COM

+ Tag2: 0x1

+ Sname: cifs/arc08r2en.foresta.com

+ Tag3: 0x1

+ EncPart:

+ Tag4:

- Authenticator:

+ SequenceHeader:

+ Tag0:

+ EType: aes256-cts-hmac-sha1-96 (18)

+ Tag2:

+ Cipher: ®—‹Xe¶øÌTÙ¤J’ä¢m²Ñ©{$@yöï©Î1·Æý\OÍ×V˜ø8 {oa|?š]ßÚQhAp{ÿÇ…à”}z@A@U³‘Áÿ[¡qä)×3d­íõE`U“éæØ@¢ð»ÛíûœÙæý2ôBj`áÉ›ª“õ÷Ê ^ãM²~]kÊo’!çU6Û“»Î¹ "\swµSÔ=‑¨ÜQu¾ÛSæßÄ¬{Ò#hJ-oÃ‰¦ëÿ˜û‰¸ê‘]/2ípèGæ±œiØ

KRB\_AP\_REP也包含在SMB的回复中，内容如下：

Frame: Number = 64, Captured Frame Length = 314, MediaType = ETHERNET

+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-09-39-10],SourceAddress:[00-15-5D-09-39-0B]

+ Ipv4: Src = 192.168.1.11, Dest = 192.168.1.14, Next Protocol = TCP, Packet ID = 5244, Total IP Length = 300

+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=61351, PayloadLen=260, Seq=2603305888 - 2603306148, Ack=2185087963, Win=513 (scale factor 0x8) = 131328

+ SMBOverTCP: Length = 256

- SMB2: R SESSION SETUP (0x1), SessionFlags=0x0

SMBIdentifier: SMB

+ SMB2Header: R SESSION SETUP (0x1),TID=0x0000, MID=0x0002, PID=0xFEFF, SID=0x0011

- RSessionSetup:

StructureSize: 9 (0x9)

+ SessionFlags: 0x0

SecurityBufferOffset: 72 (0x48)

SecurityBufferLength: 184 (0xB8)

- securityBlob:

- GSSAPI:

- NegotiationToken:

+ ChoiceTag:

- NegTokenResp:

+ SequenceHeader:

+ Tag0:

+ NegState: accept-completed (0)

+ Tag1:

+ SupportedMech: MsKerberosToken (1.2.840.48018.1.2.2)

+ Tag2:

+ OctetStringHeader:

- ResponseToken: 0x1

- MsKerberosToken: 0x1

- KerberosInitToken:

+ ApplicationHeader:

+ ThisMech: KerberosToken (1.2.840.113554.1.2.2)

- InnerContextToken: 0x1

- KerberosToken: 0x1

TokId: Krb5ApRep (0x200)

- ApRep: KRB\_AP\_REP (15)

+ ApplicationTag:

+ SequenceHeader:

+ Tag0:

+ PvNo: 5

+ Tag1:

+ MsgType: KRB\_AP\_REP (15)

+ Tag2: 0x1

- AuthorizationData:

+ SequenceHeader:

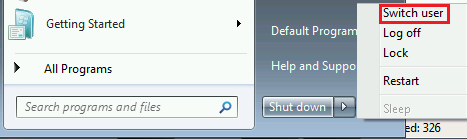
+ Tag0:

+ EType: aes256-cts-hmac-sha1-96 (18)

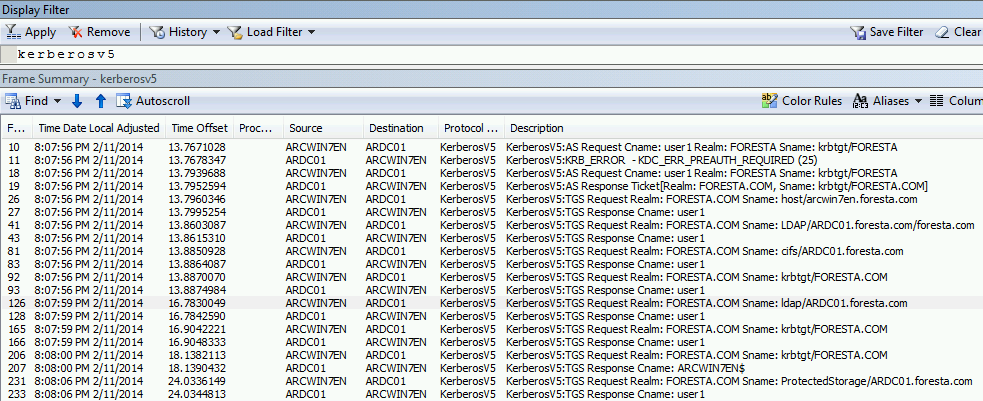
+ Tag2:

+ Cipher: ‑§ãÑ©°`q-ü[iç¿U.Ìe¤ÞpxÍTÖ2‑©ßLvS=ÖZN®2:Ã)ý2§mÐªÙOBÎC#®Þ×UÛ¨º4v¥nûa@$}ªì>êx·M8%)Æ

1. 抓取登陆网络包，查看Kerberos验证流程
2. 采用Administrator登陆ARCWin7EN，开启网络抓包
3. 点击Switch User



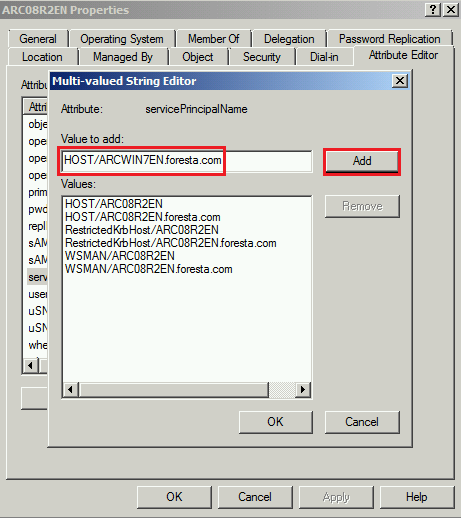
1. 采用另一个账户User1登陆，登陆后再Switch User回到Administrator的Session，停止网络抓包
2. 采用Kerberosv5过滤网络包（参考M08\_Lab\_3.cap网络包）



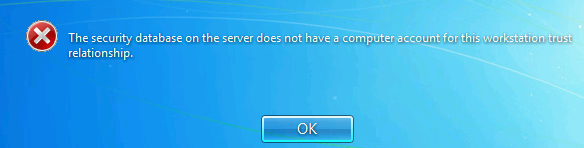
其中第一次AS Request返回KDC\_ERR\_PREAUTH\_REQUIRED(35)是由于第一次提供的请求中没有提供PaData: PA-ENC-TIMESTAMP (2)，即加密的客户端时间，因此DC要求再次提供。

之后可以看到申请了host/arcwin7en.foresta.com的服务票据（登陆）以及其他组策略需要的票据。

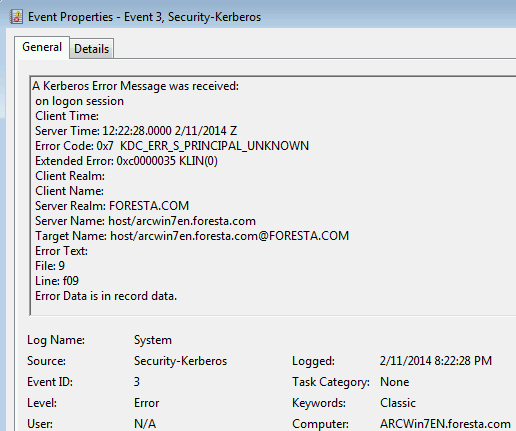
1. 设置重复SPN，查看登陆错误并排查
2. 在ADUC中，选择另一个计算机账号，添加SPN host/arcwin7en.foresta.com



1. 采用实验3中的抓包方法再次抓包，发现user1登陆错误



1. 查看网络包，发现错误KDC\_ERR\_S\_PRINCIPAL\_UNKNOWN（参考M08\_Lab\_4.cap网络包）
2. 查看系统日志，发现Kerberos 错误3

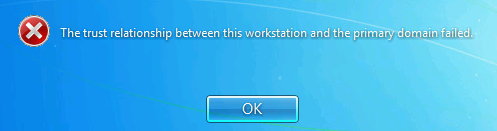


1. 采用命令setspn -x查找重复的SPN

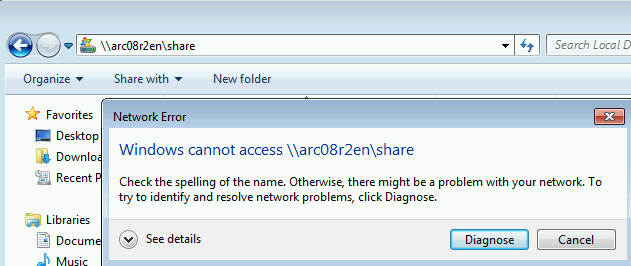


此外，也可以删除ARCWin7EN上的所有SPN以及删除计算机账号（域中没有SPN host/arcwin7en.foresta.com），都可以重现上述问题。

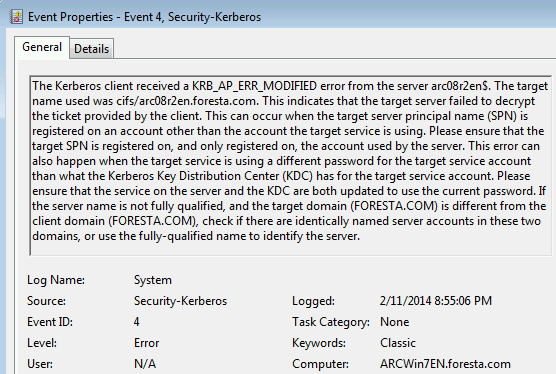
1. 设置SPN在错误的账号上，查看登陆错误并排查
2. 按照实验4的方法，在其他计算机账号上设置SPN host/arcwin7en.foresta.com，同时删除ARCWin7EN上的SPN host/arcwin7en.foresta.com。此时域中尽管只有一个SPN host/arcwin7en.foresta.com，但是注册在错误的机器上。
3. 采用实验3中的抓包方法再次抓包，发现user1登陆错误



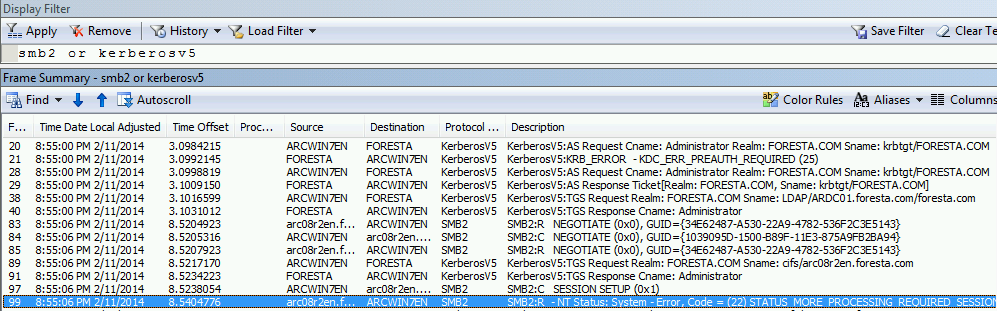
1. 查看网络包，此时不会发现Kerberos报错，这是因为本地登录，错误记录在KRB\_AP\_REP中被包含在LSA中处理。我们将在实验6中进一步确认该错误。
2. 设置SPN在错误的账号上，查看共享访问并排查
3. 把ARC08R2EN的host/arc08r2en.foresta.com删除并添加到其他计算机账号ARCWin7EN上，此时域中只有ARCWin7EN拥有该SPN。
4. 仿照实验1的方式，清空缓存并开启抓包，由Administrator账号访问[\\arc08r2en\share](file:///\\\\arc08r2en\\share)，观察如下报错



1. 查看系统日志，发现Kerberos错误4



1. 查看抓包，过滤smb2 or kerberosv5，发现错误KRB\_AP\_ERR\_MODIFIED



错误内容如下：

Frame: Number = 99, Captured Frame Length = 256, MediaType = ETHERNET

+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-09-39-10],SourceAddress:[00-15-5D-09-39-0B]

+ Ipv4: Src = 192.168.1.11, Dest = 192.168.1.14, Next Protocol = TCP, Packet ID = 8668, Total IP Length = 242

+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=61966, PayloadLen=202, Seq=2555942753 - 2555942955, Ack=3929352922, Win=513 (scale factor 0x8) = 131328

+ SMBOverTCP: Length = 198

- SMB2: R - NT Status: System - Error, Code = (22) STATUS\_MORE\_PROCESSING\_REQUIRED SESSION SETUP (0x1), SessionFlags=0x0

SMBIdentifier: SMB

+ SMB2Header: R SESSION SETUP (0x1),TID=0x0000, MID=0x0002, PID=0xFEFF, SID=0x003D

- RSessionSetup:

StructureSize: 9 (0x9)

+ SessionFlags: 0x0

SecurityBufferOffset: 72 (0x48)

SecurityBufferLength: 126 (0x7E)

- securityBlob:

- GSSAPI:

- NegotiationToken:

+ ChoiceTag:

- NegTokenResp:

+ SequenceHeader:

+ Tag0:

+ NegState: accept-incomplete (1)

+ Tag1:

+ SupportedMech: MsKerberosToken (1.2.840.48018.1.2.2)

+ Tag2:

+ OctetStringHeader:

- ResponseToken: 0x1

- MsKerberosToken: 0x1

- KerberosInitToken:

+ ApplicationHeader:

+ ThisMech: KerberosToken (1.2.840.113554.1.2.2)

- InnerContextToken: 0x1

- KerberosToken: 0x1

TokId: Krb5Error (0x300)

- Error: KRB\_ERROR (30)

+ ApplicationTag:

+ SequenceHeader:

+ Tag0:

+ PvNo: 5

+ Tag1:

+ MsgType: KRB\_ERROR (30)

+ Tag4:

+ Stime: 02/11/2014 12:55:06 UTC

+ Tag5:

+ SuSec: 370602

+ Tag6:

+ ErrorCode: KRB\_AP\_ERR\_MODIFIED (41)

+ Tag9:

+ Realm: FORESTA.COM

+ TagA:

+ Sname: arc08r2en$