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ARC08R2EN上安装Network Monitor

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

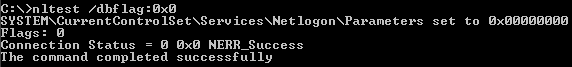
1. 抓取正常访问共享网络包，查看NTLM验证流程
2. 登陆ARC08R2EN和ARDC08R2EN，采用管理员权限打开命令行，运行如下命令开启netlogon debug日志：

nltest /dbflag:0x2080ffff



1. 在ARC08R2EN上开启网络抓包
2. 登陆ARCWin7EN，打开Windows Explorer，访问[\\192.168.1.11\share](file://192.168.1.11/share)
3. 停止ARC08R2EN上的网络抓包
4. 在ARC08R2EN和ARDC08R2EN上运行如下命令停止netlogon日志

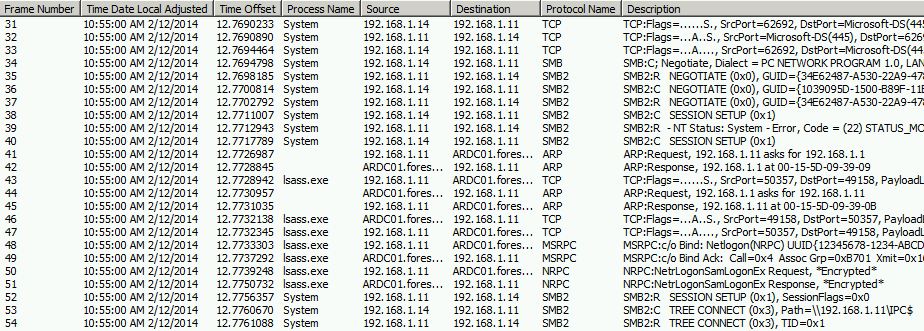
nltest /dbflag:0x0



1. 在ARC08R2EN上，查看c:\windows\debug\netlogon.log，可以观察到如下记录：



查看网络包，查看NTLM验证流程：（参考M08\_Lab\_7.cap）



SSPI Negotiate:

客户端发送支持的Negotiate方式给服务器：

Frame: Number = 34, Captured Frame Length = 213, 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 = 22727, Total IP Length = 199

+ Tcp: Flags=...AP..., SrcPort=62692, DstPort=Microsoft-DS(445), PayloadLen=159, Seq=355606016 - 355606175, Ack=666252396, Win=513 (scale factor 0x8) = 131328

+ SMBOverTCP: Length = 155

- Smb: C; Negotiate, Dialect = PC NETWORK PROGRAM 1.0, LANMAN1.0, Windows for Workgroups 3.1a, LM1.2X002, LANMAN2.1, NT LM 0.12, SMB 2.002, SMB 2.???

Protocol: SMB

Command: Negotiate 114(0x72)

+ NTStatus: 0x0, Facility = FACILITY\_SYSTEM, Severity = STATUS\_SEVERITY\_SUCCESS, Code = (0) STATUS\_SUCCESS

+ SMBHeader: Command, TID: 0xFFFF, PID: 0xFEFF, UID: 0x0000, MID: 0x0000

- CNegotiate:

WordCount: 0 (0x0)

ByteCount: 120 (0x78)

+ Dialect: PC NETWORK PROGRAM 1.0

+ Dialect: LANMAN1.0

+ Dialect: Windows for Workgroups 3.1a

+ Dialect: LM1.2X002

+ Dialect: LANMAN2.1

+ Dialect: NT LM 0.12

+ Dialect: SMB 2.002

+ Dialect: SMB 2.???

服务器返回Prefer的方式：

Frame: Number = 35, Captured Frame Length = 306, 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 = 13239, Total IP Length = 292

+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=62692, PayloadLen=252, Seq=666252396 - 666252648, Ack=355606175, Win=513 (scale factor 0x8) = 131328

+ SMBOverTCP: Length = 248

- SMB2: R NEGOTIATE (0x0), GUID={34E62487-A530-22A9-4782-536F2C3E5143}

SMBIdentifier: SMB

+ SMB2Header: R NEGOTIATE (0x0),TID=0x0000, MID=0x0000, PID=0x0000, SID=0x0000

- RNegotiate:

StructureSize: 65 (0x41)

+ SecurityMode: 1 (0x1)

DialectRevision: (0x2ff) - SMB2 wildcard revision number.

Reserved: 0 (0x0)

ServerGuid: {34E62487-A530-22A9-4782-536F2C3E5143}

+ Capabilities: 0x7

MaxTransactSize: 1048576 (0x100000)

MaxReadSize: 1048576 (0x100000)

MaxWriteSize: 1048576 (0x100000)

SystemTime: 02/12/2014, 02:55:00.965108 UTC

ServerStartTime: 02/07/2014, 05:14:52.831500 UTC

SecurityBufferOffset: 128 (0x80)

SecurityBufferLength: 120 (0x78)

Reserved2: 541936672 (0x204D4C20)

- securityBlob:

- GSSAPI:

- InitialContextToken:

+ ApplicationHeader:

+ ThisMech: SpnegoToken (1.3.6.1.5.5.2)

- InnerContextToken: 0x1

- SpnegoToken: 0x1

+ ChoiceTag:

- NegTokenInit:

+ SequenceHeader:

+ Tag0:

+ MechTypes: Prefer Negoex (1.3.6.1.4.1.311.2.2.30)

+ Tag3:

+ NegHints:

之后，客户端发送空的域名和用户名给服务器：

Frame: Number = 38, Captured Frame Length = 220, 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 = 22729, Total IP Length = 206

+ Tcp: Flags=...AP..., SrcPort=62692, DstPort=Microsoft-DS(445), PayloadLen=166, Seq=355606283 - 355606449, Ack=666252900, Win=511 (scale factor 0x8) = 130816

+ SMBOverTCP: Length = 162

- 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: 74 (0x4A)

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 NLMP (1.3.6.1.4.1.311.2.2.10)

+ Tag2:

+ OctetStringHeader:

- MechToken: NTLM NEGOTIATE MESSAGE

- NLMP: NTLM NEGOTIATE MESSAGE

Signature: NTLMSSP

MessageType: Negotiate Message (0x00000001)

+ NegotiateFlags: 0xE2088297 (NTLM v2128-bit encryption, Always Sign)

+ DomainNameFields: Length: 0, Offset: 0

+ WorkstationFields: Length: 0, Offset: 0

+ Version: Windows 6.1 Build 7601 NLMPv15

服务器返回需要更多信息进行验证：

Frame: Number = 39, Captured Frame Length = 385, 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 = 13241, Total IP Length = 371

+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=62692, PayloadLen=331, Seq=666252900 - 666253231, Ack=355606449, Win=512 (scale factor 0x8) = 131072

+ SMBOverTCP: Length = 327

- 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=0x007D

- RSessionSetup:

StructureSize: 9 (0x9)

+ SessionFlags: 0x0

SecurityBufferOffset: 72 (0x48)

SecurityBufferLength: 255 (0xFF)

- securityBlob:

- GSSAPI:

- NegotiationToken:

+ ChoiceTag:

- NegTokenResp:

+ SequenceHeader:

+ Tag0:

+ NegState: accept-incomplete (1)

+ Tag1:

+ SupportedMech: NLMP (1.3.6.1.4.1.311.2.2.10)

+ Tag2:

+ OctetStringHeader:

- ResponseToken: NTLM CHALLENGE MESSAGE

- NLMP: NTLM CHALLENGE MESSAGE

Signature: NTLMSSP

MessageType: Challenge Message (0x00000002)

+ TargetNameFields: Length: 14, Offset: 56

+ NegotiateFlags: 0xE2898215 (NTLM v2128-bit encryption, Always Sign)

+ ServerChallenge: AEDA21D108CEEA63

Reserved: Binary Large Object (8 Bytes)

+ TargetInfoFields: Length: 154, Offset: 70

+ Version: Windows 6.1 Build 7601 NLMPv15

TargetNameString: FORESTA

- AvPairs: 7 pairs

+ AvPair: FORESTA (Server NetBIOS domain name)

+ AvPair: ARC08R2EN (Server NetBIOS computer name)

+ AvPair: foresta.com (The FQDN (2) of the domain.)

+ AvPair: ARC08R2EN.foresta.com (The fully qualified domain name (FQDN (1)) of the computer.)

+ AvPair: foresta.com (The FQDN (2) of the forest.)

+ AvPair: 2:55:00 AM 2/12/2014 (Server local time)

+ AvPair: NULL

此时客户端再次发送包含更多信息的请求（NTLMv2）：

Frame: Number = 40, Captured Frame Length = 697, 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 = 22730, Total IP Length = 683

+ Tcp: Flags=...AP..., SrcPort=62692, DstPort=Microsoft-DS(445), PayloadLen=643, Seq=355606449 - 355607092, Ack=666253231, Win=510 (scale factor 0x8) = 130560

+ SMBOverTCP: Length = 639

- SMB2: C SESSION SETUP (0x1)

SMBIdentifier: SMB

+ SMB2Header: C SESSION SETUP (0x1),TID=0x0000, MID=0x0003, PID=0xFEFF, SID=0x007D

- CSessionSetup:

StructureSize: 25 (0x19)

VcNumber: 0 (0x0)

+ SecurityMode: 1 (0x1)

+ Capabilities: 0x1

Channel: 0 (0x0)

SecurityBufferOffset: 88 (0x58)

SecurityBufferLength: 551 (0x227)

PreviousSessionId: 0 (0x0)

- securityBlob:

- GSSAPI:

- NegotiationToken:

+ ChoiceTag:

- NegTokenResp:

+ SequenceHeader:

+ Tag0:

+ NegState: accept-incomplete (1)

+ Tag2:

+ OctetStringHeader:

- ResponseToken: NTLM AUTHENTICATE MESSAGEVersion:v2, Domain: FORESTA, User: Administrator, Workstation: ARCWIN7EN

- NLMP: NTLM AUTHENTICATE MESSAGEVersion:v2, Domain: FORESTA, User: Administrator, Workstation: ARCWIN7EN

Signature: NTLMSSP

MessageType: Authenticate Message (0x00000003)

+ LmChallengeResponseFields: Length: 24, Offset: 146

+ NtChallengeResponseFields: Length: 324, Offset: 170

+ DomainNameFields: Length: 14, Offset: 88

+ UserNameFields: Length: 26, Offset: 102

+ WorkstationFields: Length: 18, Offset: 128

+ EncryptedRandomSessionKeyFields: Length: 16, Offset: 494

+ NegotiateFlags: 0xE2888215 (NTLM v2128-bit encryption, Always Sign)

+ Version: Windows 6.1 Build 7601 NLMPv15

+ MessageIntegrityCheck: 4AD149D3B9E283575E972F9B511F4897

DomainNameString: FORESTA

UserNameString: Administrator

WorkstationString: ARCWIN7EN

+ LmChallengeResponseStruct: 000000000000000000000000000000000000000000000000

+ NTLMV2ChallengeResponse: 956A00E37B9B0C6845855D94E86350D5

+ SessionKeyString: C12091C158780B5A9AF78EEB8B46BF4D

+ Tag3:

+ OctetStringHeader:

+ MechListMic: Version: 1

之后服务器发送上述信息给域控进行验证，这些信息都是加密的：

48 10:55:00 AM 2/12/2014 12.7733303 lsass.exe 192.168.1.11 ARDC01.foresta.com MSRPC MSRPC:c/o Bind: Netlogon(NRPC) UUID{12345678-1234-ABCD-EF00-01234567CFFB} Call=0x4 Assoc Grp=0x0 Xmit=0x16D0 Recv=0x16D0 {MSRPC:16, TCP:15, IPv4:1}

49 10:55:00 AM 2/12/2014 12.7737292 lsass.exe ARDC01.foresta.com 192.168.1.11 MSRPC MSRPC:c/o Bind Ack: Call=0x4 Assoc Grp=0xB701 Xmit=0x16D0 Recv=0x16D0 {MSRPC:16, TCP:15, IPv4:1}

50 10:55:00 AM 2/12/2014 12.7739248 lsass.exe 192.168.1.11 ARDC01.foresta.com NRPC NRPC:NetrLogonSamLogonEx Request, \*Encrypted\* {MSRPC:16, TCP:15, IPv4:1}

51 10:55:00 AM 2/12/2014 12.7750732 lsass.exe ARDC01.foresta.com 192.168.1.11 NRPC NRPC:NetrLogonSamLogonEx Response, \*Encrypted\* {MSRPC:16, TCP:15, IPv4:1}

之后服务器返回验证成功：

Frame: Number = 52, Captured Frame Length = 159, 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 = 13246, Total IP Length = 145

+ Tcp: Flags=...AP..., SrcPort=Microsoft-DS(445), DstPort=62692, PayloadLen=105, Seq=666253231 - 666253336, Ack=355607092, Win=509 (scale factor 0x8) = 130304

+ SMBOverTCP: Length = 101

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

SMBIdentifier: SMB

+ SMB2Header: R SESSION SETUP (0x1),TID=0x0000, MID=0x0003, PID=0xFEFF, SID=0x007D

- RSessionSetup:

StructureSize: 9 (0x9)

+ SessionFlags: 0x0

SecurityBufferOffset: 72 (0x48)

SecurityBufferLength: 29 (0x1D)

- securityBlob:

- GSSAPI:

- NegotiationToken:

+ ChoiceTag:

- NegTokenResp:

+ SequenceHeader:

+ Tag0:

+ NegState: accept-completed (0)

+ Tag3:

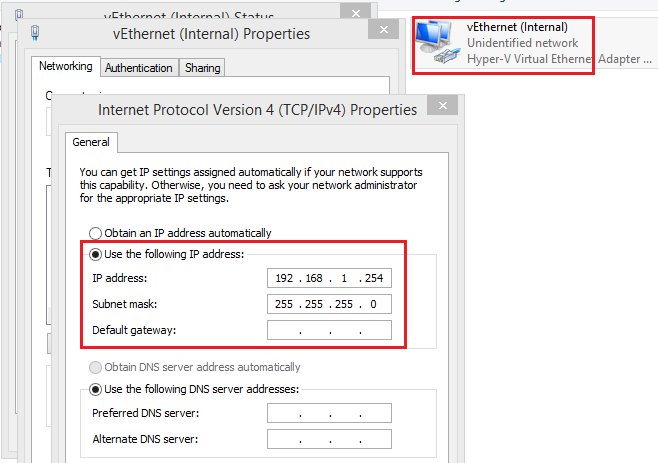
+ OctetStringHeader:

+ MechListMic: Version: 1

1. 在域控的Netlogon debug日志上查看如下记录：



1. 从Hyper-V主机访问虚拟机共享，查看网络包
2. 设置Hyper-V主机上虚拟机使用的网卡



1. 在Hyper-V主机上采用[\\192.168.1.11\share](file://192.168.1.11/share)访问虚拟机共享并抓包

此时注意到弹出验证框，输入虚拟机 的域和域名，即可访问。

此时可以发现不同域的机器可以相互访问，即使没有trust。（Hyper-V主机在公司的fareast域，而虚机在自己创建的域中。）

因此，在NTLM验证中，系统是不会检查域名，只会验证用户名和密码，及时客户端提供了域名。

1. 此外，也可以自己尝试两台未加域的机器，如果他们的Administrator用户名和密码相同，则可以直接访问共享。