

NTLM Restrictions

Liraz Barak - Microsoft PFE

NTLM Introduction

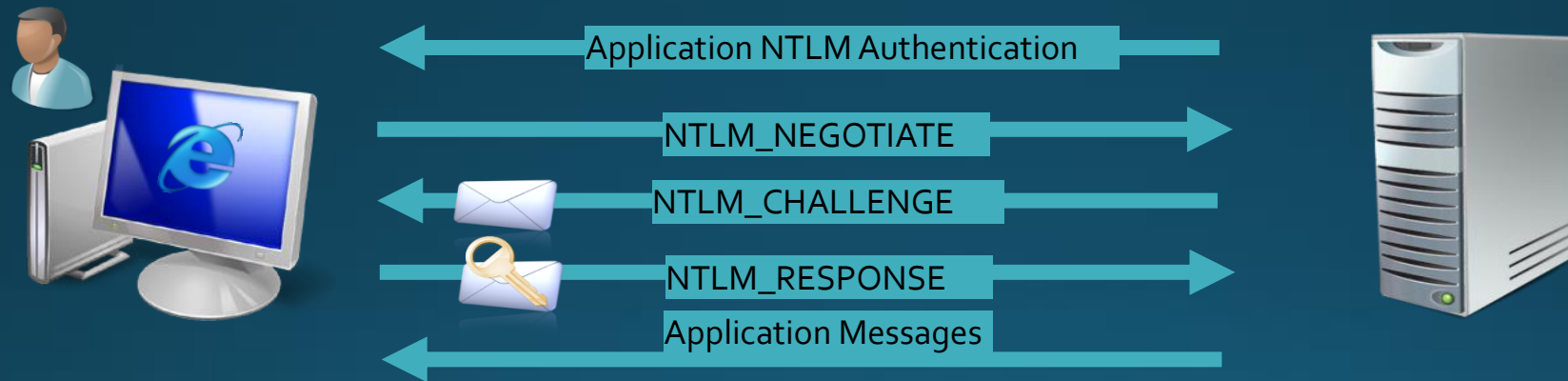
- Challenge-Response
- LM, NTLMv1, NTLMv2 all use the same message transmission protocol but differ in the response function and the computation of the password hash used as the encryption key.

LM – DES

NTLMv1 – MD4

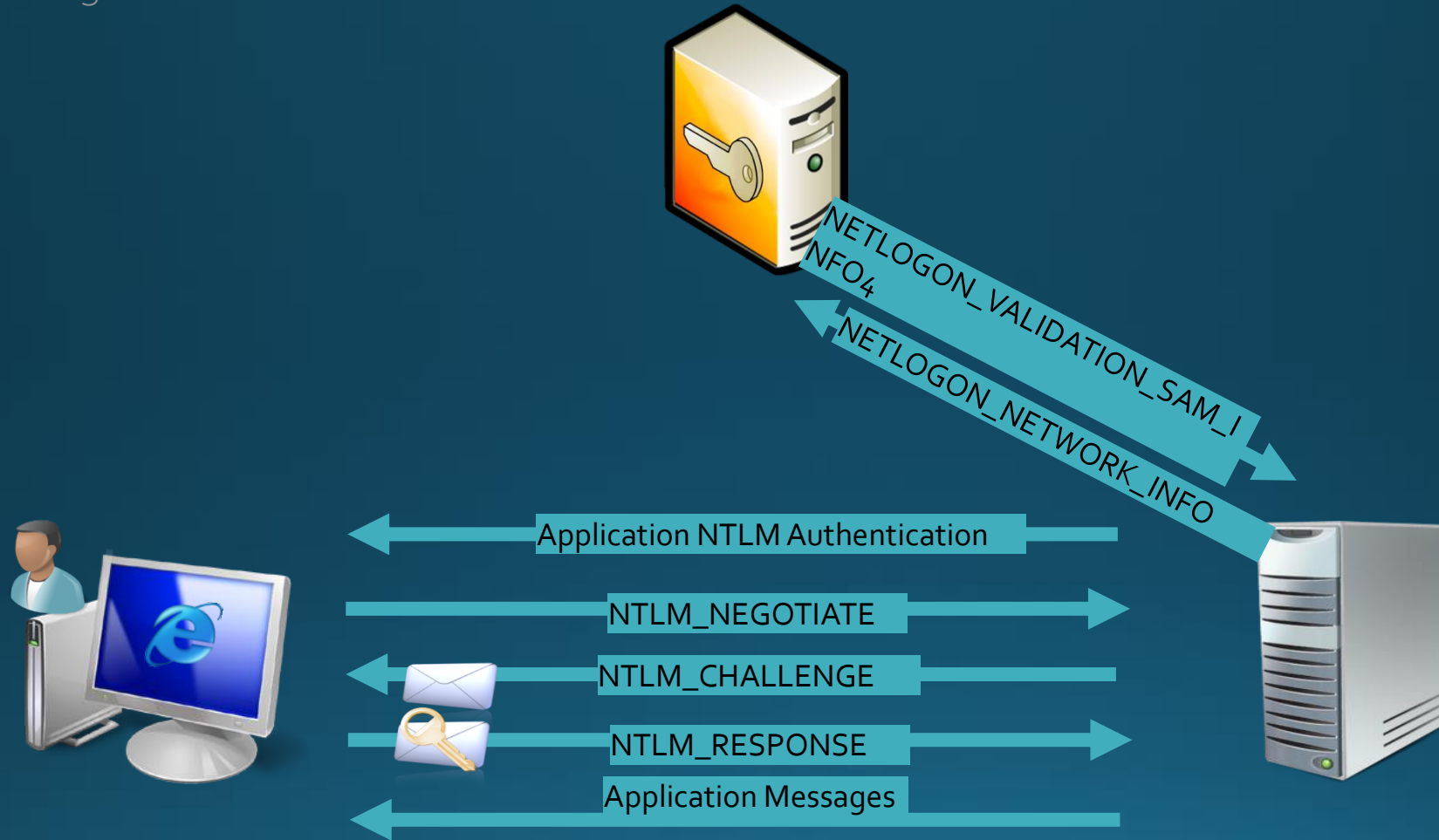
NTLMv2 – HMAC-MD5

NTLM – Message Flow (local user)



NTLM – Message Flow (domain user)

NTLM Pass-Through Authentication



NTLM – NEGOTIATE_MESSAGE

Client to Server

- Singanture = "NTLMSSP\0"
- Message Type = 0x00000001
- Negotiate Flags
- Domain Name Fields
- Workstation Name Fields
- Version
- Payload that contains:
 - Domain Name – client authentication domain name.
 - Workstation Name – client machine name.

NTLM – CHALLENGE_MESSAGE

Server to Client

- Singanture = "NTLMSSP\0"
- Message Type = 0x00000002
- Target Name Fields
- Negotiate Flags
- Server challenge (64-bit nonce)
- Reserved – always 0
- Target Info Fields
- Version
- Payload that contains:
 - Target Name – domain or machine name of the server.
 - Target Info

NTLM – AUTHENTICATE_MESSAGE

Client to Server

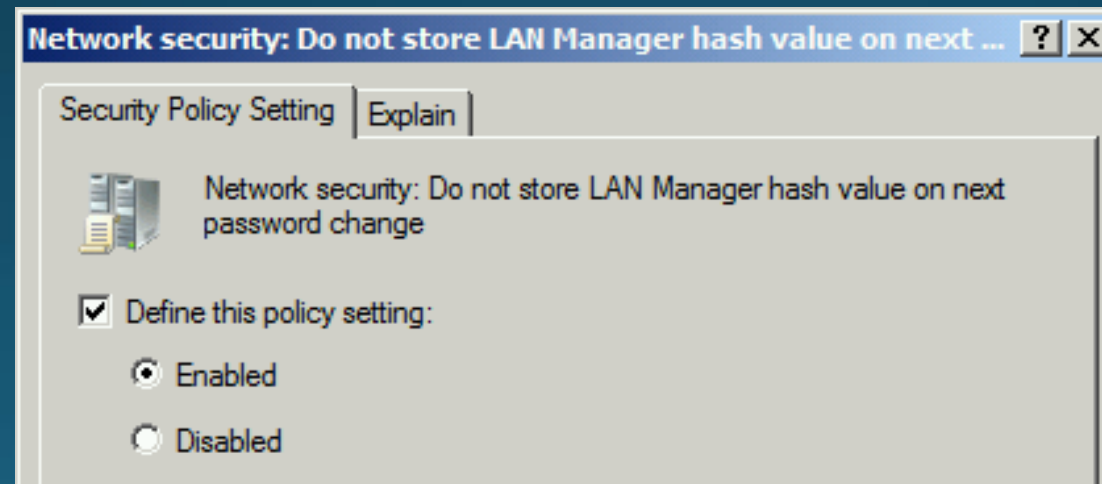
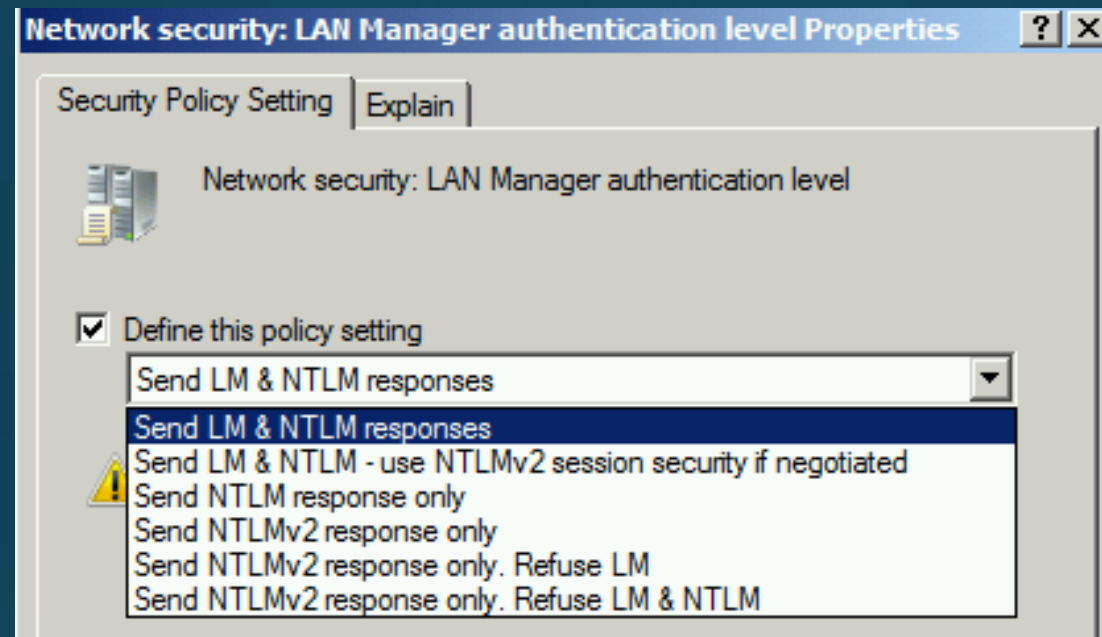
- Singanture = "NTLMSSP\0"
- Message Type = 0x00000003
- LM Challenge Response Fields
- NT Challenge Response Fields
- Domain Name Fields
- User Name Fields
- Workstation Fields
- Encrypted Random Session Key Fields
- Negotiate Flags
- Version
- MIC – message integrity

NTLM – AUTHENTICATE_MESSAGE (continued)

Client to Server

- Payload that contains:
 - LM Challenge Response – 24 bytes
 - NT Challenge Response – 24 bytes
 - Domain Name – The name of the domain or machine to which the user account belongs.
 - User Name – The user name to be authenticated.
 - Workstation – The name of the client workstation.
 - Encrypted Random Session Key

NTLM - Configuration



Advantages of Kerberos over NTLM

- Standard protocol RFC 1510/4120
- The client connects to the DC
- Faster! Using tickets cache
- Supports delegation
- Mutual Authentication
- Stronger cryptographic algorithms
- New features are added in new OS versions

NTLM – Use Cases

- Pre-Windows 2000 machines don't support Kerberos.
- Application is not Kerberos compatible and is hard-coded to use NTLM.
- The server or client are not part of a domain.
- Kerberos isn't configured correctly (missing SPN)
- Accessing the server using its IP address
- Accessing a server in a different domain (forest) with external trust.

Troubleshooting: Logging

- Kerberos

[HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]

"LogLevel"=dword:1

Kerberos trace in %windir%\system32\lsass.log

See event entries in the System EventLog

- KDC






[HKLM\SYSTEM\CurrentControlSet\Services\Kdc]

"LogLevel"=dword:1

See event entries in the System EventLog

NTLM Restrict

Group Policy – Security Options

 Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	
 Network security: Restrict NTLM: Add server exceptions in this domain	
 Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Enable auditing for all accounts
 Network security: Restrict NTLM: Audit NTLM authentication in this domain	Enable all
 Network security: Restrict NTLM: Incoming NTLM traffic	Allow all
 Network security: Restrict NTLM: NTLM authentication in this domain	Disable
 Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Audit all

Duplicate SPNs

The KDC encountered duplicate names while processing a Kerberos authentication request. The duplicate name is HTTP/www.treyresearch.com (of type DS_SERVICE_PRINCIPAL_NAME). This may result in authentication failures or downgrades to NTLM. In order to prevent this from occurring remove the duplicate entries for HTTP/www.treyresearch.com in Active Directory.

Log Name:	System	Logged:	6/13/2014 1:25:18 PM
Source:	Kerberos-Key-Distribution-C	Task Category:	None
Event ID:	11	Keywords:	Classic
Level:	Error	Computer:	ContosoDC.contoso.com
User:	N/A		
OpCode:	Info		
More Information:	Event Log Online Help		

Missing SPN

A Kerberos Error Message was received:
on logon session
Client Time:
Server Time: 19:32:39.0000 6/15/2014 Z
Error Code: 0x7 KDC_ERR_S_PRINCIPAL_UNKNOWN
Extended Error:
Client Realm:
Client Name:
Server Realm: CONTOSO.COM
Server Name: HTTP/www.treyresearch.com
Target Name: HTTP/www.treyresearch.com@CONTOSO.COM
Error Text:
File: 9
Line: f09
Error Data is in record data.

Log Name:	System	Logged:	6/15/2014 10:32:39 PM
Source:	Security-Kerberos	Task Category:	None
Event ID:	3	Keywords:	Classic
Level:	Error	Computer:	ContosoClient.contoso.com
User:	N/A		

Modified SPNs

The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server contosoiiis\$. The target name used was HTTP/contosoiiis.contoso.com. This indicates that the target server failed to decrypt the ticket provided by the client. This can occur when the target server principal name (SPN) is registered on an account other than the account the target service is using. Please ensure that the target SPN is registered on, and only registered on, the account used by the server. This error can also happen when the target service is using a different password for the target service account than what the Kerberos Key Distribution Center (KDC) has for the target service account. Please ensure that the service on the server and the KDC are both updated to use the current password. If the server name is not fully qualified, and the target domain (CONTOSO.COM) is different from the client domain (CONTOSO.COM), check if there are identically named server accounts in these two domains, or use the fully-qualified name to identify the server.

Log Name:	System	Logged:	6/9/2014 4:45:04 PM
Source:	Security-Kerberos	Task Category:	None
Event ID:	4	Keywords:	Classic
Level:	Error	Computer:	ContosoClient.contoso.com
User:	N/A		
OpCode:	Info		

Demos