NTLM Restrictions

Liraz Barak - Microsoft PFE

NTLM Introduction

- Challenge-Response

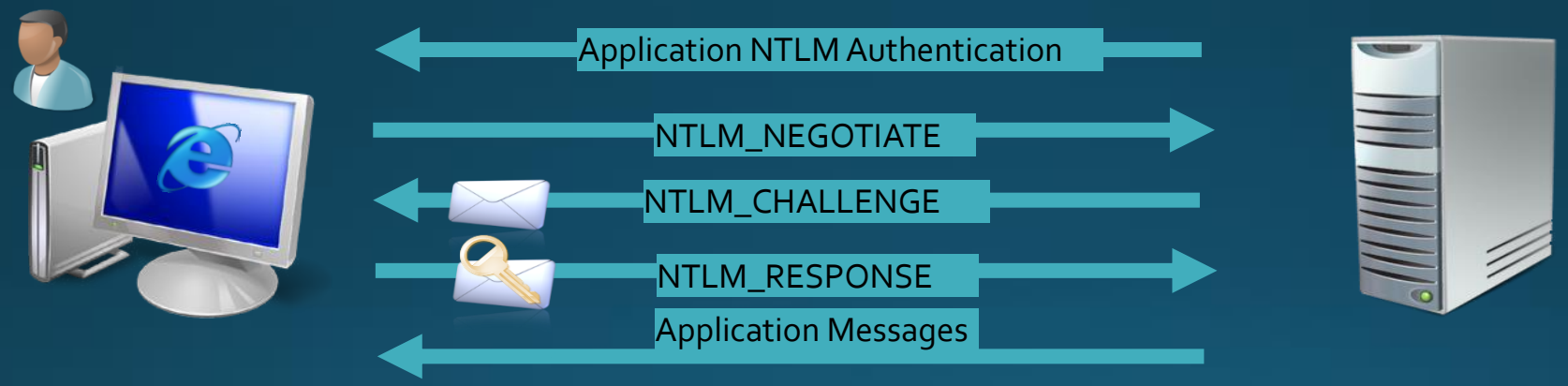
- LM, NTLMv1, NTLMv2 all use the same message transmission protocol but differ in the response function and the computation of the password hash used as the encryption key.

LM – DES

NTLMv1 – MD4

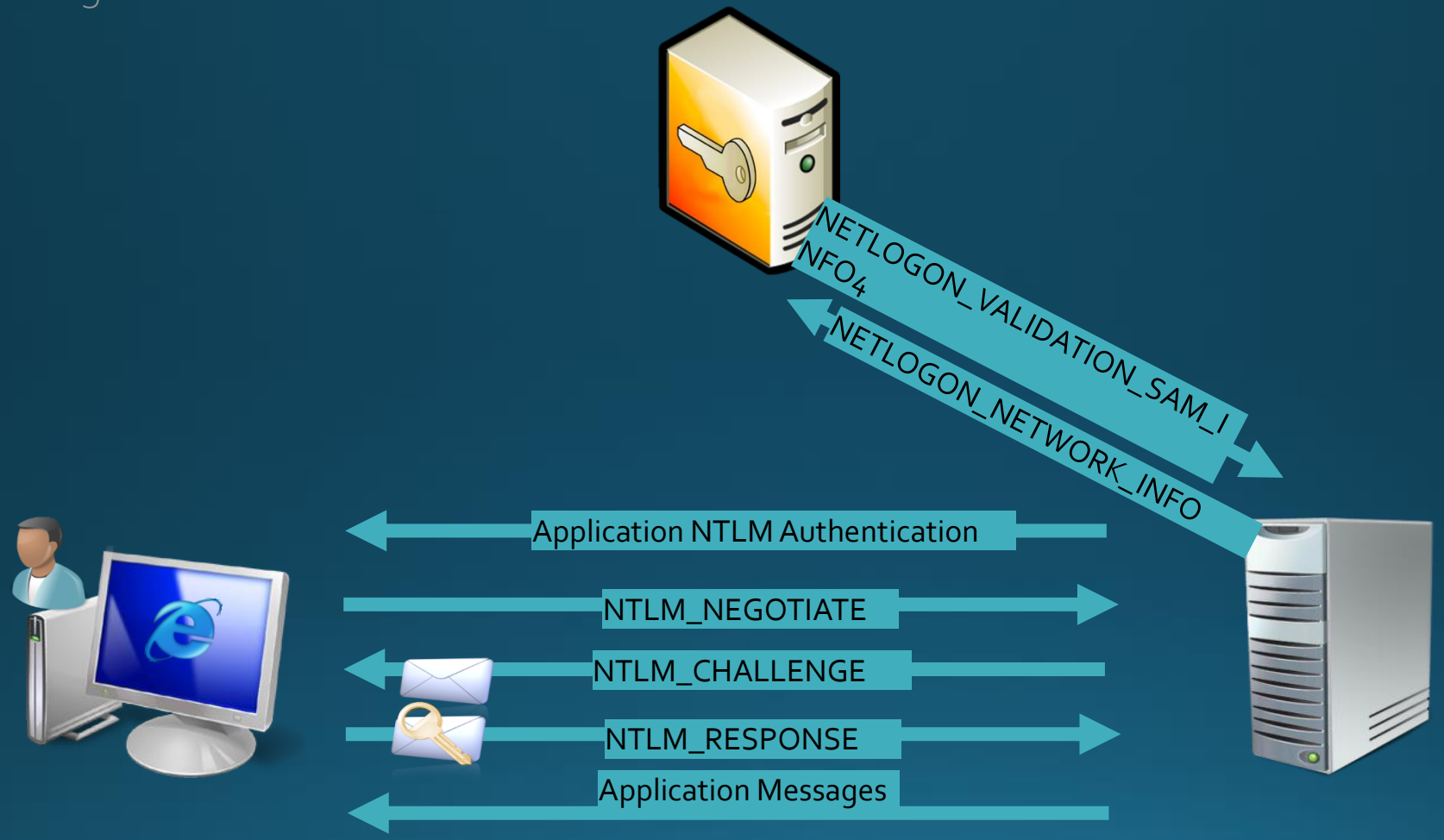
NTLMv2 – HMAC-MD5

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

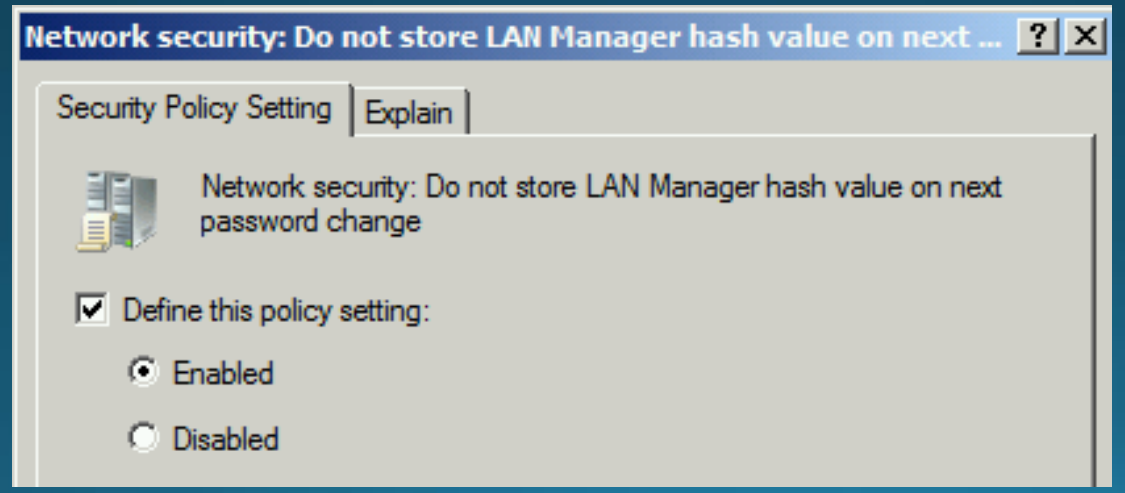
- Singanture = “NTLMSSP\0”
- Message Type = 0x00000003
- LM Challenge Response Fields
- NT Challenge Response Fields
- Domain Name Fields
- User Name Fields
- Workstation Fields
- Encrypted Random Session Key Fields
- Negotiate Flags
- Version
- MIC – message integrity

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

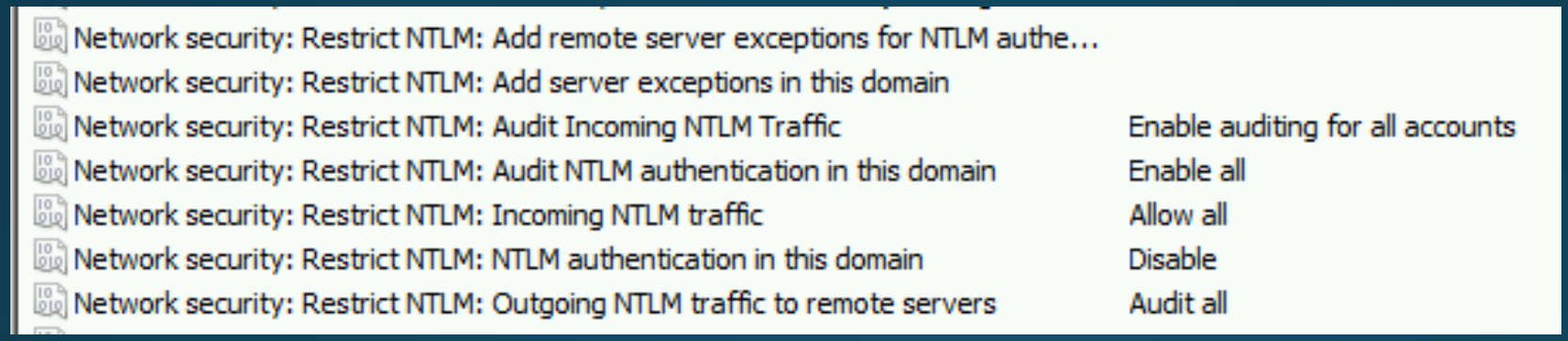
- KDC

  ```
  [HKLM\SYSTEM\CurrentControlSet\Services\Kdc]
      "LogLevel"=dword:1
  ```

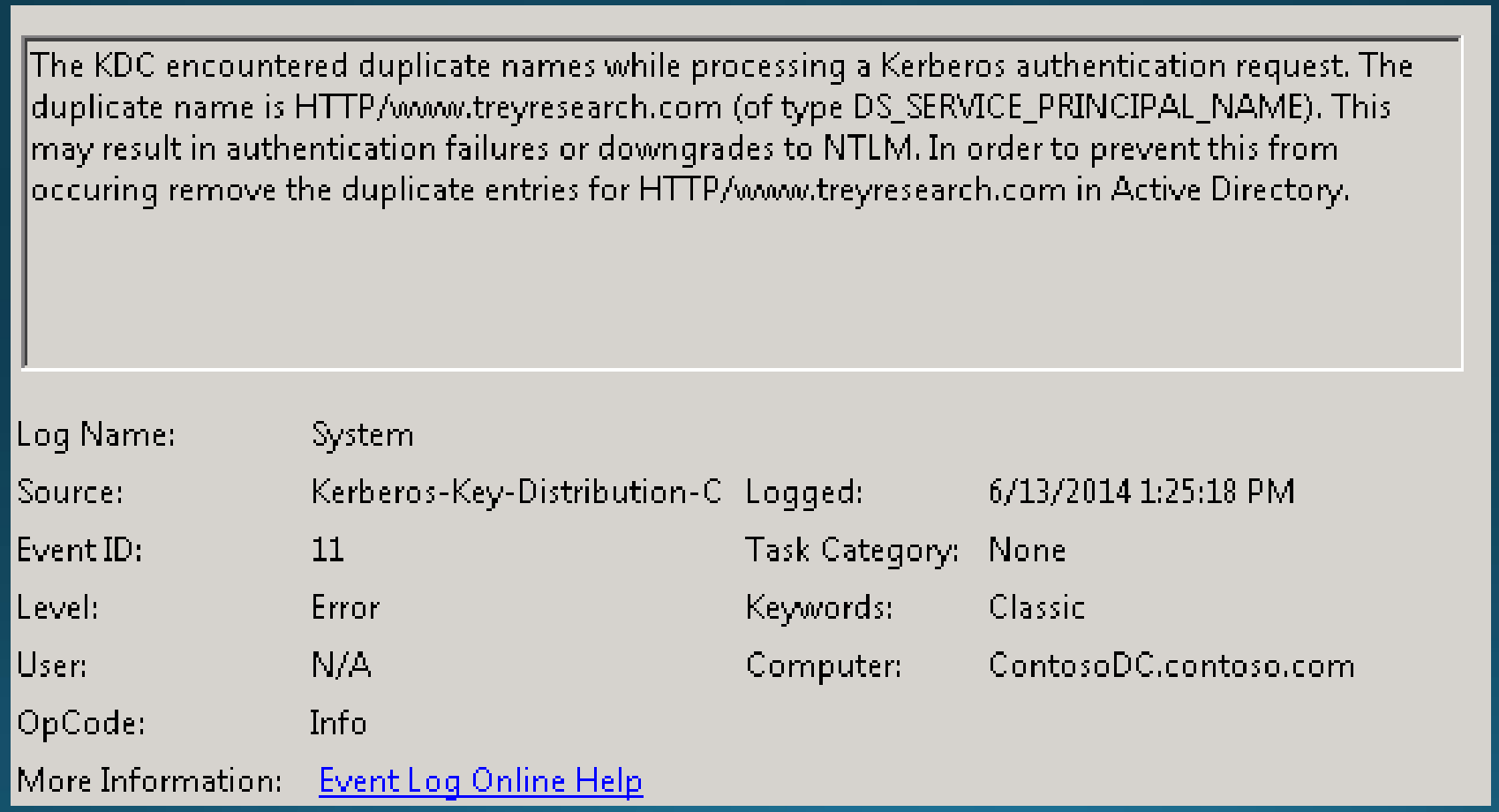
  See event entries in the System EventLog

NTLM Restrict

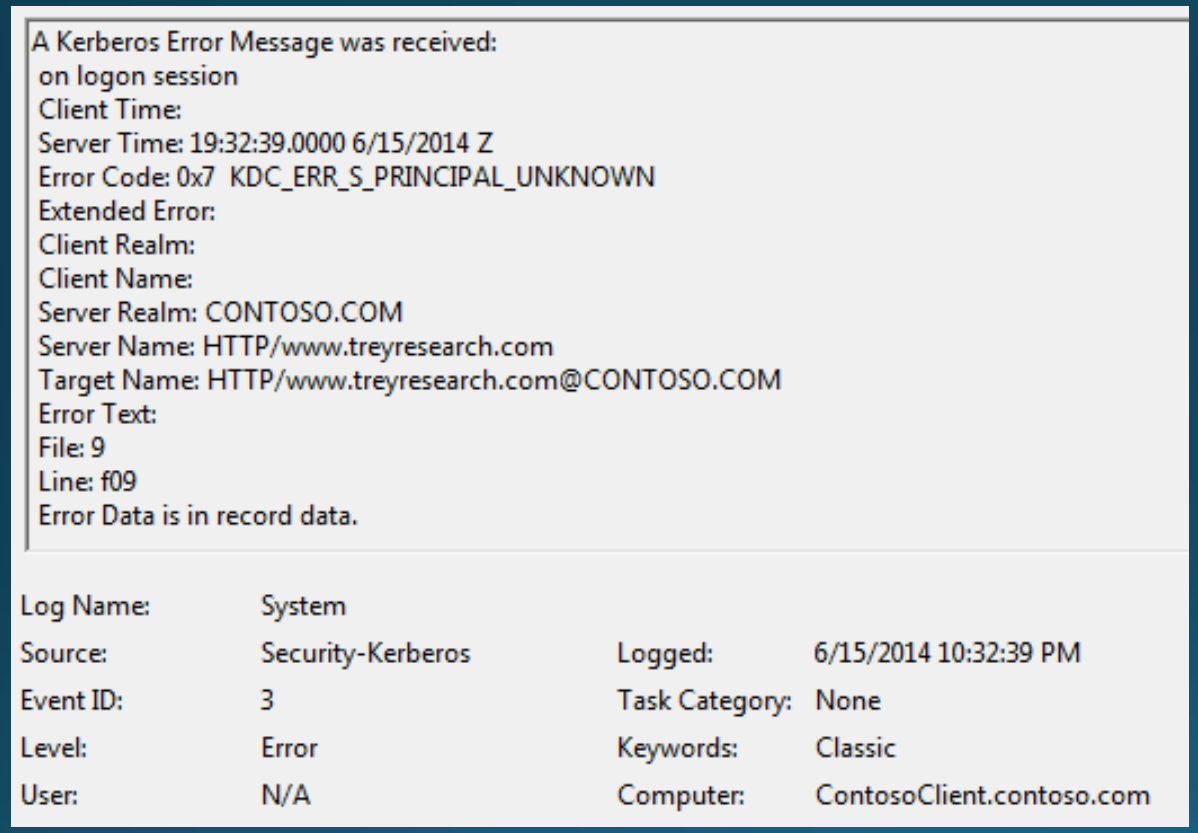
Group Policy – Security Options



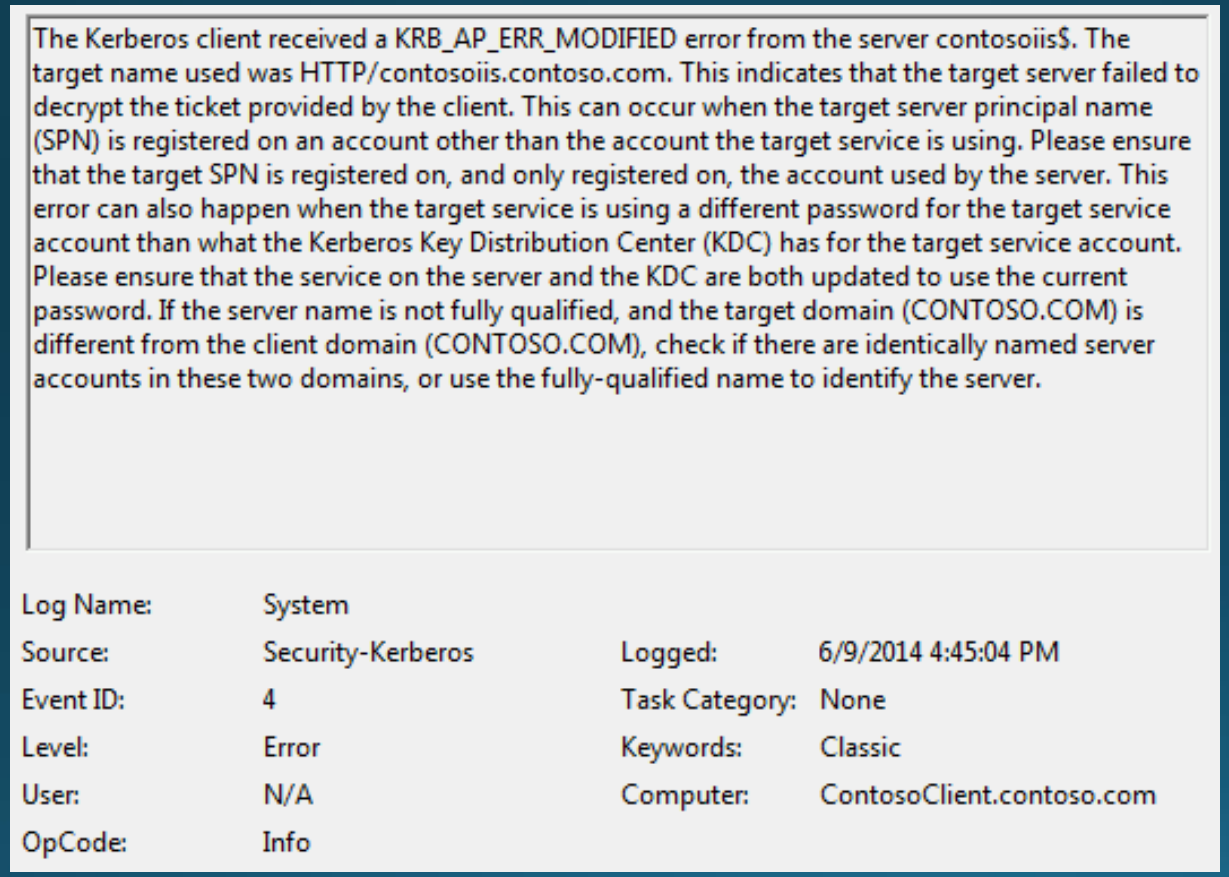
Duplicate SPNs



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

Modified SPNs



Demos