제목 : 윈도우 2000 인증 방법 및 사용자 계정 유출

윈도우 2000 에서 인증 방식은 아래 4 가지 방식이 지원이 된다. 인증 방식에 따라 서버에 지원 방식이 약간의 차이가 있으며, 보안에 최적화 인증은 커버로스 라고 할 수 있으며 AD 을 사요해야만 받을 수 있는 단점이 제공된다. 그렇기 않고는 NTLM v2 방식으로 인증이 최고의 방식이라고 할수 있다.

1. Kerberos - 액티브 디렉터리 존재시 가능
2. NTLM - 액티브 디렉터리 존재시 와 무관한 상태에서의 인증, 윈도우 2000 독립 실행형 서버시 사용됨
3. LM - 하위버전의 LAN Manager
4. Clear-Text - 유닉스 방식과 동일

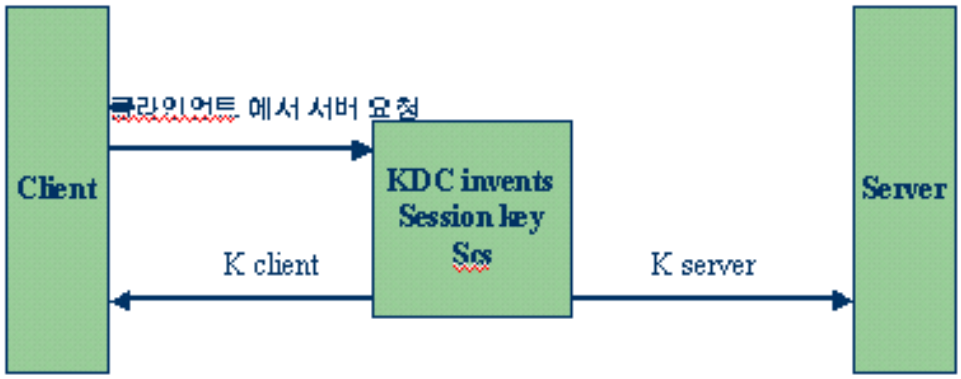
그외 인증 방식에 대한 정의 및 몇가지 알아 두어야 할 사항들을 정리 하겠다.

목차

1. 커버로스 프로토콜Kerberos(또는 Cerberus) 고대 그리스 신화의 인물
   - 윈도우 2000 클라이언트에서만 제공 되는 프로토콜
   - 클라이언트와 서버간 또는 하나의 서버와 다른 서버간에 네트워크 연결이 개방되기 전에 상호 인증을 위한 방법
   - Kerberos 프로토콜은 인증 방법은 두 사람만 아는 비밀이 있으며 이들 중 한 사람은 다른 사람이 비 밀을 알고 있는지 확인 함으로써 이 사람은 식별 할 수 있다.

- Kerberos(또는 Cerberus) 고대 그리스 신화의 인물이다. 지옥문을 지키는 머리가 3개 달린 사나운 개입니다.
- 문지기 Kerberos 처럼 프로토콜인 Kerberos 에는 세개의 머리가 있다. 이것은 클라이언트, 서버, 두 매체간을 중개하는 신뢰할 만한 제 3자이다.
- 프로토콜에서 신뢰할 만한 매개자를 Key Distribution Center(KDC) 라고 한다.

2. 커버로스 키 배포 방법



[그림. 커버로스 키 배포 방법]

KDC (Kerberos Key Distribution Center)

1.KDC 는 윈도우 2000 도메인에서 제공되며, 이것은 모든 사용 사용자에 대한 계정 정보가 있는 데이터베이스를 관리 한다.

2.사용방법은 각 보안 사용자에 대한 다른 정보와 함께 KDC 는 보안 사용자와 KDC 만 알고 있는 암호화 키를 저장 한다.

3.이 키(암호화 키)는 보안 사용자와 KDC 간의 정보 교환에 사용되며 장기 키라고 한다.

위 그림에 대한 설명

1.클라이언트에서는 서버와 대화 하려고 할때 클라이언트는 KDC 에 요청을 보낸다.

2.KDC 는 두 상대방이 서로를 인증 할때 사용할 고유한 단기간의 세션 키를 배포를 한다.

3.서버의 세션 키 사본은 서버의 장기 키로 암호화 한다.

4.클라이언트의 세션 키 사본은 클라이언트의 장기 키로 암호화 한다.

- 위에서 원하는 주소로 도착을 했는지는 확인 하지 않으며, KDC 의 메시지가 잘못된 곳에 도착 하더라도 별다른 해가 제공 되지 않는다
- 클라이언트의 비밀 키를 알고 있는 사람만 클라이언트의 세션 키 암호를 해독 가능하며, 서버 또한 마찬가지다.

3. NTLM 및 NTLM v2 개요윈도우 NT 4.0 에서는 SP4 이상에서 NTLMv2 인증을 지원 함

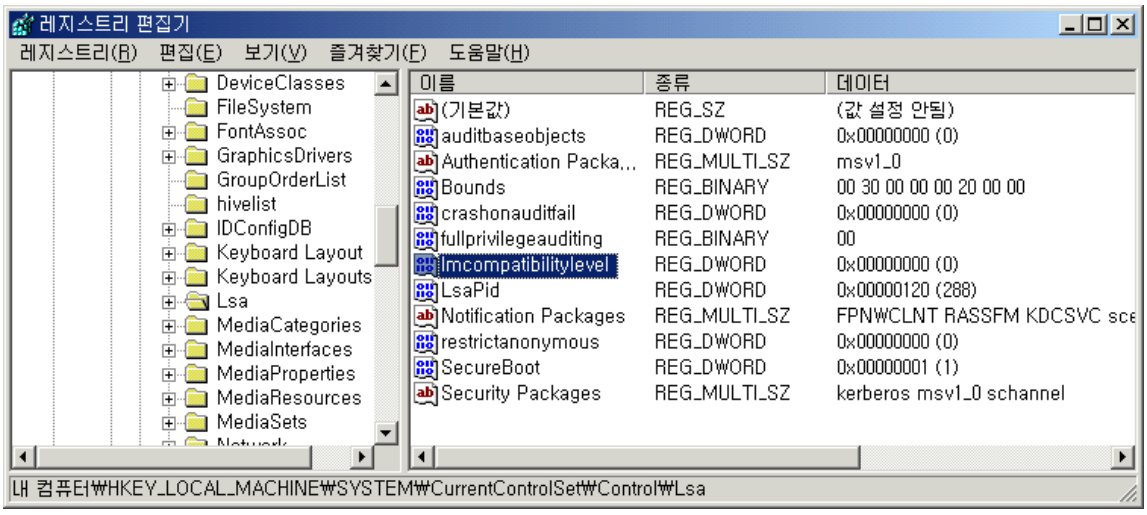
- NTLM 방식의 취약점을 보안 하고자 NTLM v2 로 업데이트 되었음
- 다운 레벨 클라이언트 인증 방식으로 커버로스 인증을 지원하지 않는 클라이언트 사용자에게 최고의 보안 인증 방식(윈도우 95, 98, NT 4.0 클라이언트)
- 도메인에 참여 하지 않는 프로토콜 사용시 가능

- 윈도우 95/98 클라이언트에서 NTLM v2 설치을 해야함(윈도우 2000 CD 에서 제공 됨)

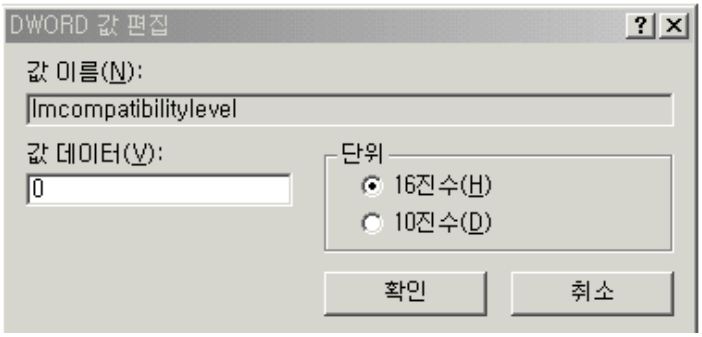
4. 윈도우 95/98 클라이언트에서 NTLM v2 설치 방법
   - 윈도우 2000 CD 에서 제공 되며, CD-ROM 에서 CLIENTS/WIN9X 에서 제공 받을 수 있음
   - 윈도우 95/98 클라이언트에서 Regedit.exe 실행 후 아래에 제공 되는 값으로 작업을 변경 해 주시면 됩니다.

     HKEY_LOCAL_MACHINE₩System₩CurrentControlSet₩Control
     Value Name: LMCompatibility
     Data Type: REG_DWORD
     Value: 3
     Valid Range: 0,3

5. NTLM 인증 방식 변경레지스트리를 편집 방법 - 윈도우 2000 기반 컴퓨터의 HKLM₩System₩CurrentControlSet₩Control₩LSA₩LMCompatibilityLevel 의 레지스트리 값을 변경하여 REG-DWORD 값에 다음 6 가지 중 하나의 값을 설정하여 수행할 수 있다



[그림. 레지스트리 화면이며, 인증 방식을 변경 할수 있는 화면임]



[그림. 레지스트리 수정 화면이며 값에 따라 인증 방식이 변경됨]

- 로컬 보안 정책 수정 - 보안 설정 > 로털 정책 > 보안 옵션 > Lan Manger 보안 수준
- 인증 방식의 값
  ① 0 (LM 전달 & NTLM 응답)- LM/NTLM,NTLMv2 허용(DC)
  ② 1 (LM 전달 & NTLM 교섭될 경우 NTLMv2 세션 보안을 사용)- NTLMv2가 가능하면 NTLMv2
  ③ 2 (NTLM 응답만 보내기) - NTLM을 기본 NTLMv2가능하면 NTLMv2
  ④ 3 (NTLMv2 응답만 보내기) - NTLMv2, Others 허용(DC)
  ⑤ 4 (NTLMv2 응답만 보내기₩LM 거부)- NTLMv2, NTLM 허용(DC)
  ⑥ 5 (NTLMv2 응답만 보내기₩LM과 NTLM 거부 -NTLMv2 외에 불허

다음 6가지 중 하나의 값

① 0 (LM 전달 & NTLM 응답)- 최대한의 상호운용성을 제공한다. 모든 다운 레벨 클라이언트들이 서버에 인증할 때 LM이나 NTLM 모두 사용할 수 있다.

② 1 (LM 전달 & NTLM 교섭될 경우 NTLMv2 세션 보안을 사용)- DS 클라이언트 소프트웨어가 전개되었을 때 더 강력한 보안을 제공한다. 클라이언트 컴퓨터가 NTLMv2를 지원한다면, 이 설정은 NTLMv2의 사용이 교섭되도록 한다. DS 클라이언트 소프트웨어의 전개 과정에서 이 설정을 사용하는 것이 좋다. DS 클라이언트 소프트웨어가 설치된 클라이언트들은 NTLMv2를 사용할 것이고, 그렇다고 아직 설치되지 않은 클라이언트의 인증이 차단되지는 않는다.

③ 2 (NTLM 응답만 보내기)- 윈도우 95, 98 클라이언트의 사용을 제한하려는 윈도우 NT 네트워크에서 유용하다. 이 설정은 DS 클라이언트가 모든 윈도우 95, 98, NT 4.0 클라이언트에 전개되었다면, 모든 다운 레벨 클라이언트의 연결을 차단한다.

④ 3 (NTLMv2 응답만 보내기) - 윈도우 2000 컴퓨터가 다운 레벨 인증 요청에 대하여 NTLMv2 인증으로 응답하도록 설정한다. 모든 다운 레벨 클라이언트에 DS 클라이언트 소프트웨어가 설치되었을 때 이를 사용해야 한다. 그렇지 않으면 이러한 클라이언트들의 네트워크로의 인증은 차단될 것이다.

⑤ 4 (NTLMv2 응답만 보내기₩LM 거부)- 윈도우 2000 컴퓨터들이 다운 레벨 인증 요청에 대하여 NTLMv2 인증으로 응답하도록 설정한다. LM 인증 요청이 윈도우 2000 컴퓨터로 전달되면, 이것들은 거부되고 NTLMv2 응답은 전달되지 않는다. 이 옵션은 윈도우 2000 컴퓨터와 DS 클라이언트 소프트웨어를 사용하는 윈도우 95, 98, NT 컴퓨터로 연결을 한정할 것이다.

⑥ 5 (NTLMv2 응답만 보내기₩LM과 NTLM 거부)- NTLMv2 응답만이 전달되고, NTLMv2를 사용하지 않는 인증 요청을 거부하도록 한다. 이 옵션은 서비스 팩 4 이상이 설치되지 않은 NT 4.0 클라이언트가 서버에 연결하는 것을 방지한다. 이 시나리오에서, 윈도우 2000, SP4 이상이 설치된 윈도우 NT 4.0 클라이언트, DS 클라이언트 소프트웨어가 설치된 윈도우 NT 4.0, 95, 98 클라이언트만이 윈도우 2000 컴퓨터에 연결할 수 있다.

6. 다운 레벨 인증 방식윈도우 95, 98, NT 4.0 클라이언트에게 NTLM v2 을 사용하여 보안을 강화

■ 윈도우 2000 에서는 NTLM v2 만 사용 할 수 있도록 보안 로컬 정책을 사용하여 수정

이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안됨)
auditbaseobjects	REG_DWORD	0x00000000 (0)
Authentication Packages	REG_MULTI_SZ	msv1_0
Bounds	REG_BINARY	00 30 00 00 00 20 00 00
crashonauditfail	REG_DWORD	0x00000000 (0)
fullprivilegeauditing	REG_BINARY	00
lmcompatibilitylevel	REG_DWORD	0x00000000 (0)
LsaPid	REG_DWORD	0x00000120 (288)
Notification Packages	REG_MULTI_SZ	FPNWCLNT RASSFM KDCS
restrictanonymous	REG_DWORD	0x00000000 (0)
SecureBoot	REG_DWORD	0x00000001 (1)
Security Packages	REG_MULTI_SZ	kerberos msv1_0 schannel

[그림. 레지스트리 화면으로 NTLN 방식 인증을 변경을 제공 됨]

7. 사용자 계정 데이터 베이스 유출일반적으로 독립 실행형 서버일 경우는 모드 사용자 데이터 베이스를 SAM 에 존재

■ ₩₩systemroot₩repair 존재

■ 시스템 운영중일때는 SAM 데이터 베이스는 유출이 되지 않는다.

■ 데이터 베이스 해독 툴로 사용자 계정을 해독 가능

이름	크기	종류
autoexec.nt	1KB	NT 파일
config.nt	3KB	NT 파일
default	120KB	파일
ntuser.dat	120KB	DAT 파일
sam	20KB	파일
secsetup.inf	573KB	설치 정보
security	28KB	파일
setup.log	156KB	텍스트 문서
software	6,396KB	파일
system	1,088KB	파일

[그림. ₩₩systemroot₩repair 디렉터리 화면 리스트]

8. 사용자 계정 데이터 베이스 해독 방법 LC3 으로 검사 하는 방법

=> http://www.atstake.com/research/lc3/index.html

User Name	LM Passw...	<8	NTLM Password	LM Hash	NT
admin	1	x	1	C2265B23734E0DACAAD3B435B51404EE	69
admin2	1	x	1	C2265B23734E0DACAAD3B435B51404EE	69
admin3	1	x	1	C2265B23734E0DACAAD3B435B51404EE	69
Administrator	1234	x	1234	B757BF5C0D87772FAAD3B435B51404EE	7C

이 기능에 대한 정보와 자료는 추후 자세한 설명과 pwdump2 와 함께 작업해서 좀더 체계적인 자료를 제공하겠다.

9. 윈도우 NT 4.0 에 응급 복구 디스크로 노출 될 수 있는 상황

NT 4.0 응급 복구 디스크는 SAM 데이터를 디스크에 백업을 받게 되며 그러면서 쉽게 사용자 계정에 대한 노출이 쉬었다. 그러면서 응급 복구 받은 디스크를 아무곳에 놓게 되었으며, 그러면서 발생 하는 것은 문제가 많았다. 아무리 syskey 로 암호화가 되어 있다 하더라도 쉽게 LC3 이라는 유사한 프로그램으로 해시를 할 수 있었기 때문이다.
Syskey 에 대해서는 아래 참조하시길 바란다.

그외 윈도우 2000 매거진에 난 기사 중에 왜 NT 의 패스워드는 취약한가 라는 기사가 제공된 적이 있다. 인용 하자면
첫째, NTLM 의 패스워드는 대소문자의 구분이 없다. 사용자가 대문자와 소문자를 섞어서 패스워드를 사용한다고 해도 NT 는 NTLM 해시를 만들기 전에 해당 패스워드를 모두 대문자로 변환 하고 해시를 만든다고 한다.
둘째,패스워드를 14 글자까지만 제공 할 수 있지만, 7 글자 이상의 패스워드의 보안이 취약하긴 마찬가지라고 한다. NTLM 에서는 7 자 이상의 패스워드를 만들기 위해 2 개의

해시를 만든다고 한다. 처음 한 개는 7 글자의 첫번째 해시를 만들고, 나머지 글자들로 두번째 해시를 만든다.
그러면서 NTLM 방식의 대한 SP 4 이상에서는 NTLM V2 로 해결 하고자 했으며, 이 방식은 클라이언트가 크랙에 취약한 NTLM 방식을 전송하지 않게 설정 된 인증 방식이다.

파일 이름	내용
Autoexec.nt	*%systemroot%*₩System32₩Autoexec.nt 파일의 복사본. MS-DOS 창을 열었을 때 초기화 파일로 사용된다.
Config.nt	*%systemroot%*₩System32₩Config.nt 파일의 복사본 MS-DOS 창을 열었을 때 초기화 파일로 사용된다.
Default._	HKEY_USERS₩DEFAULT 레지스트리 키가 압축된 파일.
Ntuser.DA_	%systemroot%₩Profiles₩Default User₩Ntuser.dat. 의 압축된 버전.
Sam._	HKEY_LOCAL_MACHINE₩SAM 레지스트리 키가 압축된 파일. 사용자 계정정보와 보안관련 사항이 유지되어 있다.
Security._	HKEY_LOCAL_MACHINE₩SECURITY 레지스트리 키가 압축된 파일.
Setup.log	설치된 파일에 대한 로그. 복구 중 사용할 CRC 정보를 가지고 있다.
Software._	HKEY_LOCAL_MACHINE₩SOFTWARE 레지스트리 키가 압축된 파일.
System._	HKEY_LOCAL_MACHINE₩SYSTEM 레지스트리 키가 압축된 파일.

[그림, 윈도우 NT 4.0 응급복구 디스크 리스트

10. SYSKEY에 방식으로 SAM 암호화에 대한 내용
윈도우 NT는 비밀번호를 일반문서로 저장 하게 될 경우는 보안상에 쉽게 노출 되므로 다음과 같은 방식으로 저장 하게 된다. 비밀번호를 먼저 해시 하게 되고, 또한 해시한 값을 다른 함수로 수정하고, 그 결과인 비밀번호 파생을 해서 SAM 데이터베이스에 저장 하는 방식이다.

해시 알고리즘 방식 - 자료를 단방향으로만 변형을 제공하는 알고리즘 방식이며, 키를 사용하는 암호화 방식과 같은 자료를 원상 복귀 시키기 위해 해시 함수를 디코딩시키거나 새로운 함수를 만들어 내는 것이 불가능 하다.
또한 암호화 시스템은 입력된 자료의 크기와 무관한 고정길이의 결과를 만들어내기 위해 해시 함수를 사용 한다.
문서에 적용 방식에 대해서는 고정길이 결과를 이용 해서 원래의 문서와 수신된 문서의 해시 값이 같다면 수신과정에서 문서가 변형되지 않았다는 것을 확인이 되며, 그렇지 않을 경우는 문서의 보안 상태를 의심해 봐야 한다.

위 두가지 방식을 보면, 사용자의 비밀번호 및 문서에 대한 적용할 수 있다는 것이다.
윈도우 2000 에서는 해시 함수를 사용 하여 비밀번호 보안에 사용을 한다.

위 글은 MS 및 윈도우 2000 매거진 기사를 참조한 내용입니다.
MS 참조 : Windows NT System Key Permits Strong Encryption of the SAM

http:// http://support.microsoft.com/support/kb/articles/q143/4/75.asp

11. 용어 정리

- MD(Message Digest) – 메시지 요약
- Cipher – 암호화를 수행하는 수학적인 알고리즘
- DES(Data Encryption Standard) – 자료 암호화 표준, 기본 56비트
- 3DES (Triple DES) – 3개 까지의 키를 사용 하고, 세단계의 계산 과정을 거치는 확장된 알고리즘
- CryptoAPI – 암호화 함수의 다양한 집합을 OS 와 함께 사용 하여 보안 애플리케이션을 만들고자 할 때 적용한다. 이 모듈에서는 관리 함수,키 생성 함수, 인증 인코드와 디코드 함수, 인증 저장 함수,메시지 암호화와 해독함수,메시지 서명 등이 포함 된다.