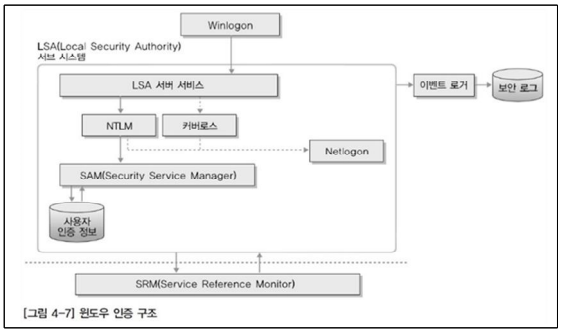
4주차 2차시. 윈도우 인증과 패스워드

【학습목표】

1. 윈도우 인증 및 패스워드 관리에 대해 설명할 수 있다.

학습내용1 : 윈도우 인증의 구성요소

1. 윈도우 인증 구조



[그림 4-7] 윈도우 인증 구조

2. 윈도우 인증의 구성요소

① LSA(Local Security Authority)
모든 계정의 로그인에 대한 검증
로컬 및 원격 시스템 자원 및 파일 등에 대한접근 권한 검사
이름과 SID를 매칭하며, SRM이 생성한 감사 로그 기록

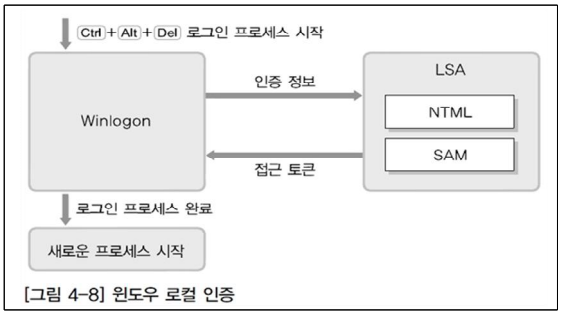
② SAM(Security Account Manager)
윈도우에서 패스워드 암호화하여 보관하는 파일의 이름과 동일
%systemroot%/system32/config/sam

③ SRM(Security Reference Monitor)
SAM이 사용자의 계정과 패스워드 일치 여부를 확인하여 알리면 사용자에게 SID(Security Identifier) 부여
SID에 기반하여 파일이나 디렉터리에 대한 접근(access) 허용 여부 결정, 이에 대한 감사 메시지 생성

학습내용2 : 로컬 인증과 도메인 인증

1. 로컬인증

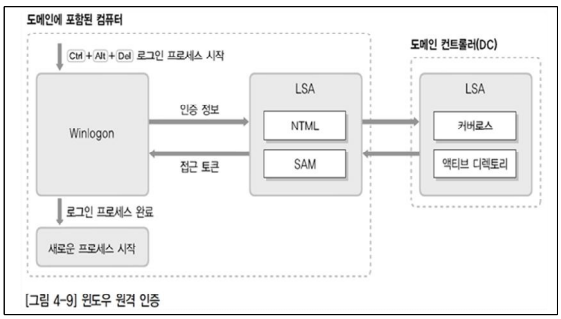
① Ctrl+Alt+Delete
② Winlogon 화면
③ 아이디와 패스워드 입력
④ LSA 서브 시스템이 인증 정보를 받아 NTML 모듈에 아이디와 패스워드 넘겨줌
⑤ SAM이 받아 확인
⑥ 로그인 허용



[그림 4-8] 윈도우 로컬 인증

2. 도메인 인증

① Ctrl+Alt+Delete
② Winlogon 화면
③ 인증 정보 입력
④ 해당 정보 LSA 서브 시스템에 인계
⑤ LSA 서브 시스템에서 해당 인증 정보가 로컬 인증용인지 도메인 인증용인지 확인
⑥ 커버로스(Kerberos) 프로토콜 이용, 도메인 컨트롤러에 인증 요청



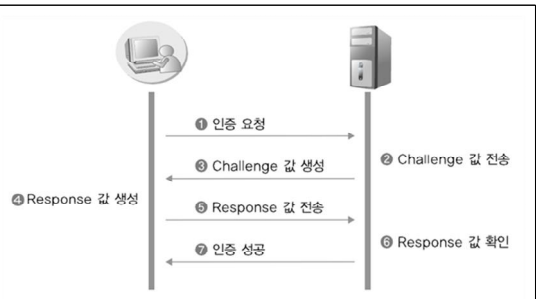
[그림 4-9] 윈도우 원격 인증

도메인 인증에서는 기본적으로 풀 도메인 이름(FQDN: Full Qualified Domain Name)과 커버로스 프로토콜을 이용하게 되어 있지만, IP를 이용해 접근을 시도할 경우NTML 사용
도메인 컨트롤러의 인증 정보를 확인
· 접속하고자 하는 사용자에게 접속 토큰 부여
· 해당 권한으로 프로세스를 실행

학습내용3 : 인증구조

1. 패스워드 값을 인증서버에 직접 전달하는 인증 방식

① 텔넷 또는 FTP 접속을 하는 경우
② 웹 포털 사이트에 로그인하는 경우
③ 단순 인증 방식은 패스워드 노출 및 재사용 공격에 취약함
④ Challenge & Response 인증을 통한 방법으로 인증을 수행해야 함



[그림 4-10] Challenge & Response 인증

2. Challenge & Response 인증

① 인증 요청
인증을 수행하고자 하는 주체가 인증 서버에 인증 요청
② Challenge 값 생성
③ Challenge 값 전송
인증 요청 받은 인증 서버는 문자열 등의 값을 특정 규칙을 따르거나 혹은 랜덤하게 생성 인증 요구자에 전달
④ Response 값 생성
인증 요구자는 서버에서 전달받은 Challenge 값과 본인이 입력한 패스워드 정보를 이용해 서버에 보낼 Response 값 생성
⑤ Response 값 전송
⑥ Response 값 확인
⑦ 인증 성공
인증 요구자는 생성한 Response 값을 인증 서버에게 전달
인증 서버는 Response 값을 확인하여 인증 요구자의 적절한 패스워드 소유 여부 확인
확인된 Response가 적절하면 인증의 성공 여부 인증 요구자에 알림

3. LM & NTLM

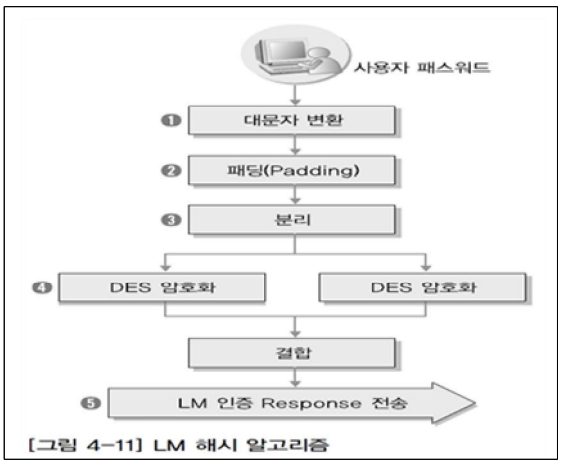
* LM(Lan Manager) 해시

1980년대에 만들어진 알고리즘으로, 본래 IBM의 OS 2에서 사용

MS에서 1993년에 만든 윈도우 NT에 탑재되기 시작

LM은 구조적으로 취약한 알고리즘

윈도우 2000, XP의 기본 알고리즘



[그림 4-11] LM 해시 알고리즘

* LM(Lan Manager) 해시 알고리즘 절차

① 대문자 변환

사용자가 패스워드 입력하면 모두 대문자로 전환

② 패딩(Padding)

기본적으로 14글자를 하나의 패스워드로 인식

14글자가 되지 않는 패스워드는 뒤에 0을 붙여 14자리로 만듦

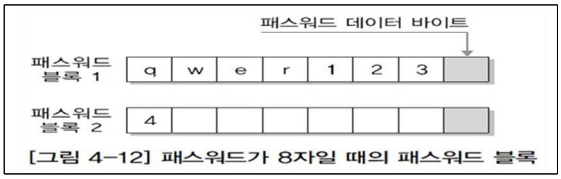
③ 분리

패스워드 길이에 관계없이 8바이트가 블록 하나를 형성

1바이트는 패스워드 블록에 대한 정보를 담고 있음

실질적 패스워드 문자열은 7바이트, 즉 문자 7개로 구성

패스워드가 qwer1234라면 8자이므로 패스워드 블록 두 개 형성



[그림 4-12] 패스워드가 8자일 때의 패스워드 블록

④ DES 암호화

두 개 블록으로 분리된 패스워드는 각각“KGS!@#$%”라는 문자열을 암호화 키(Key)로 사용해 암호화

⑤ 결합

KGS!@#$% 로 각각 암호화한 두 결과 값을 합하여 SAM 파일에 저장

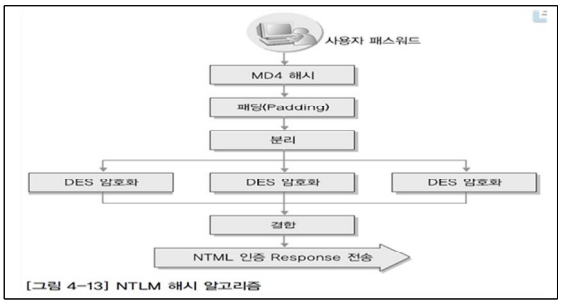
* LM(Lan Manager) 해시 한계점

qwer1234는 qwer123과 4로 나뉨

qwer123이 쉽게 크래킹 되지 않을 수도 있으나, 4는 수초 내 크래킹

4. NTLM 해시

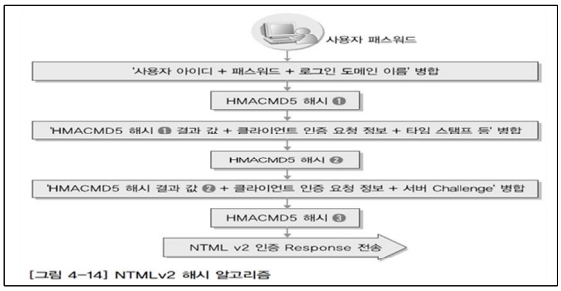
* LM 해시에 MD4 해시 추가



[그림 4-13] NTLM 해시 알고리즘

5. NTLM v2해시

* 윈도우 비스타 이후의 윈도우 시스템에서 기본 인증 프로토콜로 사용



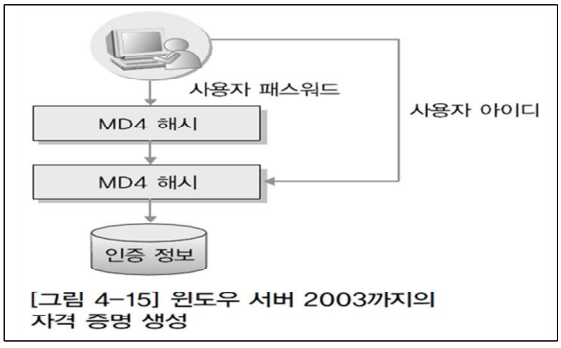
[그림 4-14] NTMLv2 해시 알고리즘

학습내용4 : 자격 증명

자격 증명(Cache Credential)이란?

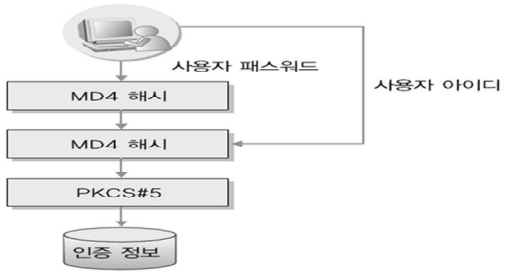
네트워크가 연결되지 않은 경우에도 도메인에 등록된 PC에 로그인할 때 도메인 계정을 사용해 로그인 할 수 있도록 하는 기능
Password verifier 라고도 함

* 윈도우 서버 2003까지의 자격 증명 생성



[그림 4-15] 윈도우 서버 2003까지의 자격 증명 생성

* 윈도우 비스타 이후 자격 증명 생성



[그림 4-16] 윈도우 비스타 이후 자격 증명 생성

【학습정리】

1. 윈도우 인증의 구성 요소는 LSA(Local Security Authority), SAM(Security Account Manager), SRM(Security Reference Monitor)가 있다.

2. Challenge & Response 인증은 인증 요청, Challenge 값 생성, Challenge 값 전송, Response 값 생성, Response 값 전송, Response 값 확인, 인증 성공의 과정을 통해 이루어진다.