MS-SQL 사용자 계정 취약점 점검 기능 설계

장승주*, 김성진*
*동의대학교 컴퓨터공학과
e-mail:sjjang@deu.ac.kr, makeitso@deu.ac.kr

Design of user account vulnerability checking function using MS-SQL

Seung-Ju Jang*, Sung-Jin Kim*
*Department of Computer Engineering, Dongeui University

요 약

본 논문은 MS-SQL 데이터베이스의 환경과 C++ 환경을 이용하여 데이터베이스 사용자 계정이 만료되었는지의 여부를 점검한다. 패스워드 혹은 사용자 설정이 변경된 시간을 체크함으로써 사용자 계정이 만료되었거나 오랫동안 패스워드를 변경하지 않았으면 보안 취약점이 존재하는 것으로 판단한다. 이것은 제 3의 악의적인 사용자가 해킹 등을 하는 것을 방지, 예방을 한다. 최근에는 정보자산이 더욱 중요시 여기게 되는 상황에서 데이터베이스의 정보 손실이 일어나게 된다면 큰 피해를 입게 된다. 본 논문은 MS-SQL 데이터베이스의 사용자 계정 만료 유무와 오랫동안 패스워드 혹은 사용자 설정이 변경되지 않은 사용자 정보를 모듈로 개발하여 보안취약점 점검을 함으로써 악의적인 사용자가 데이터베이스에 접근을 할 수 없도록 한다.

1. 서론

본 논문에서는 MS-SQL DB(Database) 보안 취약점 점검을 한다. MS-SQL 데이터베이스의 사용자 계정 만료 유무 상태와 오랫동안 사용하지 않은 계정의 패스워드가 변경되지 않았다면 악의적인 사용자나 허락되지 않은 사용자의 접근을 허용할 수 있기 때문에 보안취약점이 존재하게 된다. 이러한 문제를 해결하기 위해 데이터베이스의 사용자 계정을 체크하고 점검함으로써 보안 취약점 문제점을 해결한다.

최근 데이터베이스의 보안 취약점으로 인해 내부 비인가자 혹은 인가자의 데이터 정보 접근에 대한 통제 정책이 정상적으로 이루어지지 않아 사용자 계정 데이터 정보가 유출되는 사고가 발생하고 있다. 데이터베이스 권한부여 방식은 관리자 계정으로 데이터베이스 오브젝트에 접근할 수 있는 권한을 계정 사용자에게 부여하는 방식이다. 권한을 부여 받은 사용자 계정은 보호를 받지 못하는 몇 가지 보안취약점의 문제가 생기게 된다. 또한 대부분의 침해 사고들은 보안 시스템 부족 등의 1차적인 문제가 아닌, 부정확한 현황 파악과 보안 담당자의 시스템 관리 소홀로 인해 발생하는 경우가 대부분이며, 이는 관리자와 보안 담당자의 보안인식 부족에 기인한다. 최근의 침해사고 유형은 단순히 한 가지의 기법만이 이용되는 것이 아니라 시스템 보안취약점과 더불어 네트워크의 구성을 활용하는 등의 다양한 기법이 사용되고 있어, 사고 예방을 위해서는 최초 시스템을 구축하는 단계에서부터 보안을 고려하는 것이 점차 중요해지고 있다.

본 논문에서 개발한 MS-SQL 데이터베이스 모듈은 사용자 계정의 만료 상태 유무를 체크하고 사용자의 패스워드가 마지막으로 변경된 시간을 체크함으로써 일정 기준점 이상 해당 계정을 사용하지 않았거나 오랫동안 패스워드 혹은 사용자 설정을 변경하지 않았다면 보안취약점이 존재 할 수 있는 것으로 판단을 하여 사용자에게 경고 메시지를 보내주어 보안취약점을 예방 및 문제점을 해결할 수 있다.

본 논문의 구성은 2장에서 관련연구를 언급한다. 3장에서는 MS-SQL 보안에 대해 설명한다. 4장에서는 MS-SQL 사용자 계정 만료 및 패스워드 변경 시간 체크 프로그램을 개발하여 사용자 데이터베이스의 데이터 보안에 대해 설명한다. 5장에서는 결론을 내린다.

2. 관련 연구

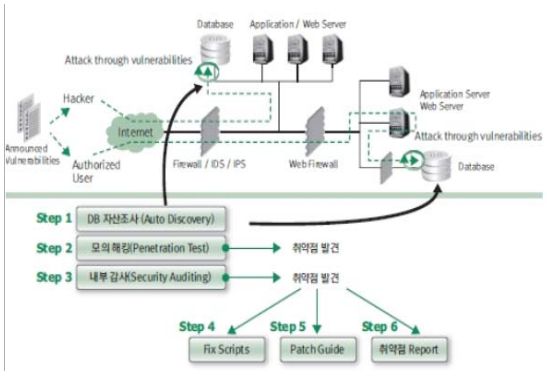
데이터베이스는 데이터와 정보를 기반으로 하는 자료의 모음으로 쉬운 접근과 관리의 목적으로 서로 다른 자료와 관계하거나 자료를 처리하기 위한 다양한 방법을 제공하는 시스템이다[1].

보안 취약점 (Vulnerability)은 좁은 의미로 컴퓨터의 하드웨어 또는 소프트웨어의 결함이나 체계 설계상의 허점으로 인해 사용자 (특히, 악의를 가진 공격자)에게 허용된 권한 이상의 동작이나 허용된 범위 이상의 정보 열람을

가능하게 하는 약점이다. 넓은 의미로는 좁은 의미에 더하여 사용자 및 관리자의 부주의나 사회공학 기법에 의한 약점을 포함한 정보체계의 모든 정보 보안상의 위험성을 말한다. 악의를 가진 공격자는 이러한 약점을 이용하여 공격 대상 컴퓨터 또는 정보화 기기에서 공격자가 의도한 동작을 수행하게 하거나 특정한 정보를 탈취한다. 보안 취약성 또는 취약성으로 부르기도 한다[2].

DB 침해 사고는 외부의 해커, 인가된 내부 사용자, 인가되지 않은 내부 사용자 등 모든 범위에서 발생할 수 있다. DB는 정보시스템의 가장 깊은 곳에서 운영되지만 웹 애플리케이션(Web Application), 내부망(internal Network), 파트너 연계 네트워크 등 수 많은 접근성의 존재로 인해 데이터 유출 위험이나 서비스 중지의 위험이 상시적으로 존재한다.

DB 취약점은 해커들에 의해 항상 공개가 된다. 이렇게 공개된 DB 취약점들을 통해 DB는 쉽게 공개 대상으로 주목된다. DB 취약점 분석은 DB에 내재된 취약점들과 DB 운영에 있어서 고려되어야 할 항목들을 다각도에서 구체적으로 점검함으로써 보안 관리자 및 DBA에게 시스템에 내재된 안전 취약점(Security Hole)을 제거하게 하여 DB의 보안 수준을 향상시키게 한다. DB 취약점 분석은 점검 대상 네트워크 범위에 존재하는 정보 자산을 파악하는 정보 수집(Information Gathering), DB 보안을 검증할 수 있는 모의해킹(Penetration Test), 내부 보안감시(Security Auditing) 등의 과정을 통해 다양한 DB 취약점들을 도출하여 DB 취약점 분석은 정보 자산의 파악과 보안성의 검토, 검출된 취약점 제거를 위한 Fix Scripts 및 개선안 제시, 레포팅 등을 주요 항목으로 한다[2][5].



(그림 1) DB 취약점 분석 절차

취약점 공격 또는 익스플로잇(exploit)이란 컴퓨터의 소프트웨어나 하드웨어 및 컴퓨터 관련 전자 제품의 버그, 보안 취약점 등 설계상 결함을 이용해 공격자의 의도된 동작을 수행하도록 만들어진 절차나 일련의 명령, 스크립트, 프로그램 또는 특정한 데이터 조작을 말하며, 이러한 것들을 사용한 공격 행위를 이르기도 한다. 취약점 공격은 주로 공격 대상 컴퓨터의 제어 권한 획득이나 서비스 거부 공격 등을 목적으로 한다[2].

취약점 공격이 만들어지는 시점은 취약점이 얼마나 널리 알려져 있는지 와는 관계없지만, 취약점 공격이 널리 공개되는 시점은 보통 해당 취약점이 널리 알려진 후 이다. 보통은 이러한 시점에 이르기 전에 해당 취약점을 보완한 업데이트가 공개되므로 항상 최신의 업데이트를 적용하여 취약점을 보완하거나 최신 버전의 바이러스 검사 등을 이용하면 위협에 대한 노출을 줄일 수 있다. 하지만 이 외의 취약점 공격의 대책은 미흡하여 여전히 보안의 위협에 노출이 될 가능성이 크다. 본 논문에서 개발한 프로그램은 사용자 계정의 만료 상태 유무를 체크하고 사용자의 패스워드가 마지막으로 변경된 시간을 체크함으로써 일정 기준점 이상 해당 계정을 사용하지 않았거나 오랫동안 패스워드 혹은 사용자 설정을 변경하지 않았다면 보안 취약점이 존재 할 수 있는 것으로 판단을 하여 사용자에게 경고 메시지를 보내주어 보안취약점을 예방 및 문제점을 해결할 수 있다. 보안 취약점 체크를 함으로써 위험성에 대한 노출을 더욱 줄일 수 있다[2][4].

3. MS-SQL 보안

IT 기술의 급속한 발전은 데이터베이스의 질적 수준 향상을 위한 정보화 추진을 가속화 하고 있지만 그 만큼 정보 보호의 한계가 나타나게 되어 나날이 데이터베이스의 보안 취약점에 대한 보안 대책이 요구되고 있다.

관리자 계정의 패스워드는 모든 보안의 가장 기본이다. 하지만 이런 기본이 지켜지지 않아 여전히 해킹사고가 많이 발생하고 있다. 패스워드 보안은 모든 보안의 기본이자 가장 중요한 필수 보안 사항이다. SQL Server sa 로그인은 서버 수준의 보안 주체로서 인스턴스를 설치하면 기본적으로 생성이 된다. SQL Server 2005 부터는 sa의 기본 데이터베이스가 master이다. 이 동작은 이전 버전의 SQL Server에서 변경되었다. 관리자 계정이 sa 계정이고 처음 설치 시 설정되는 sa 계정 패스워드는 일반 계정보다 더욱 중요시 여겨야 한다. sa 계정이 악의적인 사용자가 접근을 하게 되면 모든 계정의 데이터베이스 정보가 유출될 가능성이 크기 때문에 패스워드가 유추되지 않도록 노력해야 한다. 그러므로 관리자 계정 패스워드는 유추가 불가능하고 패스워드 크랙으로도 쉽게 알아낼 수 없는 강력한 패스워드를 사용하도록 한다. 패스워드는 길이가 최소 한 8자 이상이고, 이름이나 계정명으로 유추할 수 없는 것이어야 한다. 또한 사전에 없는 단어를 사용하도록 하고,

기호문자를 최소 한 개 이상 포함시키도록 한다[6].

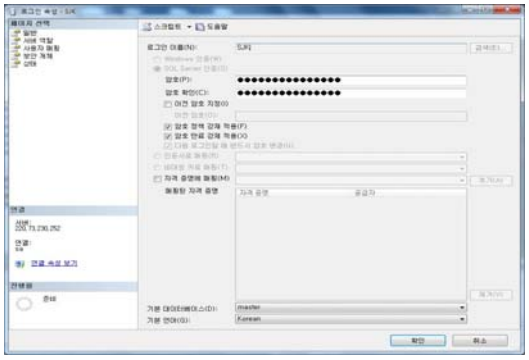
하지만 패스워드를 아무리 어렵게 설정하였다 하더라도 관리자 중에 퇴사자나 부서 이동 자가 있을 수 있고, 관리의 부주의 등으로 패스워드가 유출될 수도 있다. 또한 무작위로 대입하는 brute force 프로그램을 이용하여 일일이 패스워드를 입력해 보는 방법으로도 패스워드를 알 수 있으므로 단순히 패스워드를 추측하기 어렵게 설정하는 것만으로는 확실한 보안취약점의 문제점을 해결할 수는 없다. 그러므로 주기적인 패스워드 변경이 필요하다.

4. MS-SQL 사용자 계정 만료 기능 설계

MS-SQL는 인증 모드 사용을 통해 SQL 사용 권한이 없는 사용자로부터 비밀번호 정책을 사용하여 보안을 강화할 수 있다. 본 논문에서 개발한 MS-SQL 사용자 계정 만료 및 패스워드 변경 시간 체크 프로그램은 C++와 Microsoft SQL Server 2008 R2 기반으로 모듈화를 하여 사용자로부터 계정의 보안 상태를 편리하게 확인할 수 있도록 하여 보안을 더 강화하기 위한 목표를 두고 있다.

본 연구에서 개발한 모듈은 먼저 Microsoft SQL Server 2008R2의 SQL Server Management Studio에서 관리자 권한으로 접속을 한다. 관리자 권한으로 접속을 한 후 보안 로그인에서 사용자 설정 및 계정을 확인한다. 만약 사용자 계정의 보안이 위협을 받게 되면 제 3자 악의적인 사용자가 예상 치 못한 취약점 공격을 가하게 된다면 사용자 데이터베이스의 데이터가 손상 될 가능성이 크다. 사용자 입장에서는 보안의 취약점 판단을 하기는 문제점이 있다. 그 중 사용자의 안이한 태도가 있는데 보안 취약점 공격에 대한 대책을 하지 않고 외부에서의 접근을 방치하는 경향이 있다. 문제점 해결의 가장 간단한 방법으로는 주기적인 패스워드 변경이나 복잡한 패스워드 설정이 있는데 본 논문에서는 일정 기간 동안 패스워드를 변경하지 않으면 사용자에게 보안 취약점이 존재 한다는 경고 메시지를 보내주고 패스워드 변경을 하도록 메시지를 보내준다. 또한 오랫동안 사용하지 않는 계정이나 기간이 만료된 계정에 대해서도 보안 취약점이 존재 할 수 있기 때문에 해당 계정에 만료된 사용자가 있다면 경고 메시지를 보내어 준다.

MS-SQL의 계정 만료 사용자 및 패스워드 설정 정보를 보기 위해서는 계정 로그인 속성을 확인해야 한다. 먼저 Server 관리자 계정에 접속을 한 후 보안 로그인에서 사용자의 정보를 확인한다.



(그림 2) 사용자 로그인 속성

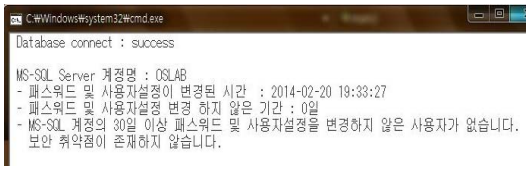
(그림 2)는 사용자 로그인 속성을 보여준다. 암호 정책 강제 적용(F)과 암호 만료 강제 적용(X)이 있는데 암호 정책을 사용하여 SQL 사용 권한이 없는 사용자로부터 접근을 제한할 수 있게 하여 보안을 강화할 수 있다. 본 논문에서는 사용자 계정 만료 상태를 먼저 체크하고, 만약 만료된 계정이 존재 한다면 사용자에게 메시지를 보내어 보안 취약점을 조금 더 예방 및 해결할 수 있다. 계정 만료 사용자를 확인한 후 오랫동안 패스워드 및 사용자 변경을 하지 않으면 보안성 문제가 존재하기 때문에 주기적으로 패스워드를 변경해 주어야 한다. 그러기 위해서는 MS-SQL의 modify_date문과 현재 시간을 받아와서 차를 계산하여 일정 기간 이상 패스워드 및 사용자 설정을 변경하지 않은 계정을 보안취약점이 존재하는 계정으로 판단하여 사용자에게 경고 메시지를 보내준다. 본 논문에서는 패스워드 및 사용자 설정이 기준점(30일) 이상 변경되지 않았다면 보안 취약점이 존재하는 것으로 판단을 하도록 설계했다. 다음 (그림 3)은 본 논문에서 개발한 MS-SQL 사용자 계정 만료 및 패스워드 변경 시간 체크 프로그램을 실행하는 첫 화면이다.

(그림 3) 프로그램 실행 성공 확인

먼저 프로그램을 실행하게 되면 관리자 계정이 정상적으로 접속을 했는지 체크한다.

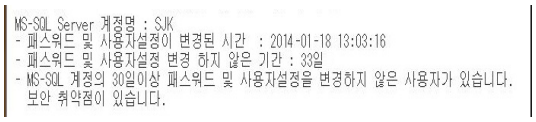
(그림 4) 인증서 기반 SQL Server 로그인

(그림 4)는 이름이 이중 해시 표시(##)로 묶인 서버 보안 주체는 내부 시스템 용도로만 사용된다. (그림 4)의 보안 주체는 SQL Server를 설치할 때 인증서에서 생성되며 삭제하면 안 된다.



(그림 5) 보안 취약점이 없는 계정

(그림 5)는 사용자의 계정이 만료되지 않았고 패스워드 변경이 30일 이상 지나지 않았기 때문에 보안 취약점이 존재하지 않는 것으로 판단한다. 현재 데이터베이스 시스템에서 가장 이상적인 화면으로 보안취약점이 존재하지 않으므로 사용자의 데이터베이스 정보가 조금 더 안전하게 보호 될 수 있다.



(그림 6) 보안취약점이 존재하는 계정

(그림 6)은 만료된 계정은 아니지만 기준점 (30일) 이상 패스워드 및 사용자설정이 변경되지 않아서 보안취약점이 있는 것으로 판단을 하여 사용자에게 경고 메시지를 보내준다. 계정이 만료된 사용자가 아니더라도 패스워드를 주기적으로 바꾸어주지 않으면 악의적인 의도를 가진 사용자가 취약점 공격을 가할 수 있다. 3장에서 말하는 유추하기 쉬운 패스워드나 여러 번 시도를 통한 패스워드 접근 등은 주기적인 패스워드 변경으로 어느 정도 문제점을 해결 할 수 있다.

5. 결론

데이터베이스 보안은 사용자로부터 조직 또는 개인의 정보 유출에 대한 방어를 목적으로 한다. 데이터베이스 보안 취약점들은 사용자의 실수나 공개된 취약점 등으로부터 기인하게 된다. 악의적인 사용자의 권한 접근으로 인해 비정상적인 접근행위를 하게 된다면 그 위험도는 사용자들에게 큰 피해를 입힐 것이다.

본 논문에서 제안하는 DB(Database) 보안 취약점 점검 기능은 MS-SQL 데이터베이스의 보안 취약점 점검을 통하여 사용자 계정 만료 상태 유무와 오랫동안 변경되지 않은 사용자 패스워드를 체크하여 일정 기준점 이상 사용하지 않은 계정이나 패스워드 변경 시간이 변경되지 않고 기준점 이상이 되면 보안취약점이 존재하는 것으로 판단을 하여 사용자에게 경고 메시지를 보내주게 된다. 이러한 기능은 데이터베이스의 보안을 조금 더 강화하고 문제점을 예방함으로 사용자들의 정보를 효율적으로 보호할 수 있다.

참고문헌

[1] KISA, “Database security audit log Specification for Personal Information protection”, Korea Information Security Agency, 2008.

[2] 장승주, 김성진 “Oracle 특정 IP 보안취약점에 관한 연구”, 한국통신학회 2014년도 동계종합학술발표회, pp.392-394, 2014.

[3] 김유경, 신승철, 안준선, 이욱세, 이은영, 한환수 “소프트웨어 보안취약점 데이터베이스 구축 사례”, 정보과학회지 제28권 제2호, pp.20-31, 2010. 02.

[4](http://www.netbuysell.co.kr/global_asp/board/board_view.aps?Codeno=5&K_no=359&Pgtype=A

[5] DB 취약점 분석 개요, DBGuide 데이터베이스 구축 운영 종합정보 (www.DBGuide.net)

[6] 웹 서버 구축 보안점검 안내서, 방송통신위원회, 한국인터넷진흥원

[7] 박현아, 이동훈, 정영택 “암호화된 데이터베이스 검색 시스템의 보안 요구사항에 대한 통합적 관점에서의 연구”, 정보보호학회논문지 제22권 제3호, pp.621-635, 2012.

[8] 김동진, 조성제 “국가 DB 기반의 국내외 보안취약점 관리 체계 분석”, internet and Information Security 제1권 제2호, pp.130-147, 2010. 11.