다양한 취약점 점검 도구를 이용한 자동화된 네트워크 취약점 통합 분석 시스템 설계*

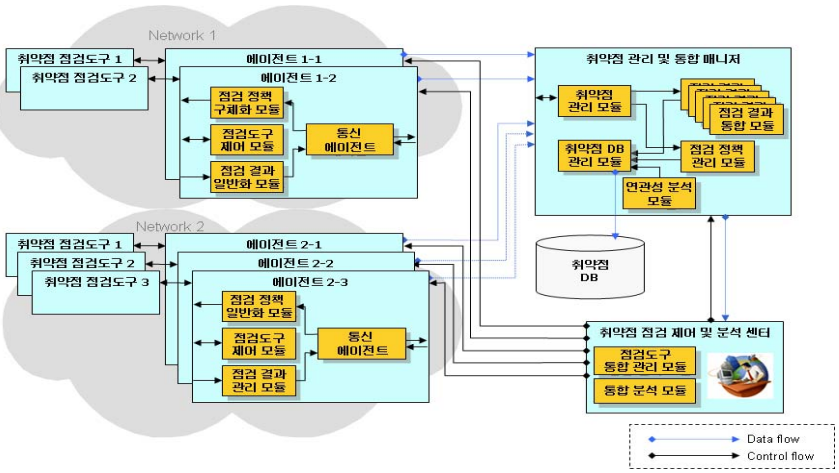
윤준○ 심원태
한국정보보호진흥원
jun@kisa.or.kr, wtsim@kisa.or.kr

Design of automatic network vulnerability analysis system using multiple heterogeneous vulnerability scanners

Jun Yoon○ WonTae Sim
Korea Information Security Agent

본 논문에서는 네트워크 취약점 분석 결과의 정확성을 향상시키기 위한 방법으로 다양한 취약점 점검 도구를 통합할 수 있는 네트워크 취약점 자동 분석 시스템(Multiple Scanner Integrated Controller& Analyzer, 이하 MSCA)을 제안한다. 일반적으로 사람에 의한 수동 점검이 가장 정확한 취약점 점검 방법으로 평가되지만, 복잡하고 규모가 큰 네트워크의 경우 효율적인 취약점 분석을 위해 자동화된 네트워크 취약점 점검 도구를 활용한다. 그런데 취약점 점검 도구의 종류에 따라 점검 대상이 다르거나, 동일한 점검 대상에 대해서도 점검 항목과 점검 결과가 다를 수가 있어, 상호보완적인 목적으로 몇 개의 취약점 점검 도구를 동시에 사용하는 방법이 활용된다. 그러나 다양한 취약점 점검 도구들의 점검 결과에 대한 연관성 분석과 통합 분석에는 사람에 의한 수동적인 분석 작업이 필요하기 때문에 상당히 시간 소모적인 작업이 되고, 네트워크의 규모에 따라 통합 분석이 불가능하기도 하다. 본 논문에서는 다양한 취약점 점검 도구를 통합할 수 있는 인터페이스를 제공하고, 공통의 점검 정책 수립과 자동화된 점검 결과 통합 분석을 특징으로 하는 시스템을 제안한다.

MSCA는 다양한 취약점 점검 도구들을 원격에서 제어하고, 점검 결과를 수집하여 통합 분석할 수 있는 구조인데, 이것은 다음 그림에서 보는 바와 같이 취약점 점검 도구 에이전트, 취약점 관리 및 통합 매니저, 취약점 점검 제어 및 분석 센터에 의해 구현된다.



<그림 1> MSCA 시스템 구성도

* 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음. [2005-S-606-02, 차세대 침해사고 예측 및 대응 기술]

MSCA의 취약점 통합 분석 절차는 3단계로 구성되는데, 다중 취약점 점검 도구에 적용이 가능한 공통의 점검 정책 수립하고 각 취약점 점검 도구별로 정책을 구체화하는 점검정책 수립 단계와 다중 취약점 점검 도구들이 점검을 수행한 후 그 결과를 수집하여 데이터베이스에 저장하는 취약점 점검 및 결과 수집 단계, 수집된 취약점 점검 결과에 대한 연관성 분석 및 통합 분석을 수행하는 점검결과 통합분석 단계이다.

이기종의 취약점 점검 도구를 원격에서 제어하고 자동화된 취약점 통합 분석을 하기 위해서는 크게 취약점 점검 정책의 일반화 문제와 취약점 점검 도구 제어 문제,취약점 점검 결과의 통합 문제를 해결해야 한다. 이중 취약점 점검 결과의 통합 문제는 다시 점검 결과 포맷의 일반화,자동화된 취약점 식별, 취약점 내용의 통합 등의 문제로 세분화된다.

취약점 점검 도구 별로 점검 정책의 표현 범위와 상세 수준이 다르다.다양한 취약점 점검 도구를 통합 관리하기 위해서는 모든 취약점 점검 도구에 적용이 가능한 공통의 점검 정책이 필요하다.본 논문에서는 다양한 취약점 점검 도구의 점검 정책 분석을 통해 일반화된 취약점 점검 정책을 정의하였다. 또한 공통의 점검 정책에 대한 히스토리 관리를 통해서 취약점 점검도구와 상관없이 취약점 점검 정책을 일관성 있게 유지할 수 있도록 하였다. 또한, 점검 도구별로 점검 정책의 범위와 상세 수준이 다르기 때문에, 공통의 점검 정책을 각 점검 도구의 정책에 맞게 구체화할 필요가 있다.공통의 취약점 점검 정책은 기본적으로 각 점검 도구의 정책과 직접 매핑이 될 수 있고,일부는 에이전트나 취약점 점검 제어 및 분석 센터에서 에뮬레이션을 통해 구현될 수 있다.

서로 다른 취약점 점검 도구들의 점검 결과를 통합 분석하기 위해서는 우선 점검 결과 포맷을 공통의 포맷으로 변환하고 상호연관성 분석을 통해 동일한 취약점을 식별하는 과정이 필요하다.본 논문에서 설명하는 연관성 분석은 이종의 보안도구에 의해 발생된 이벤트간의 연관성 분석을 통해 침해사고 판단 정확도를 향상시키고 심각도를 측정하는 다른 연구들과는 차이가 있다.본 논문은 동종의 보안제품인 취약점 점검 도구의 점검 결과에 대한 연관성 분석을 다루고 있는데,사전에 플러그인 분석을 통한 취약점 정보 매핑 방법과 공인 취약점ID에 기반한 분석 방법을 적용할 수 있다.전자의 경우 플러그인 분석에 상당한 시간과 노력이 필요하고 새로운 취약점이 발생할 때마다 분석이 필요하며,각 점검도구 개발 업체의 지원이 필요하다. 신규 취약점 발생시 신속한 보안 점검 및 대응을 위해서는 플러그인 분석에 의한 매핑 방법보다 공인 취약점ID에 기반한 연관성 분석 방법이 더 효과적이다.많은 보안 회사와 제품들이 공인 ID와 호환성이 있거나 호환성을 추진하고 있기 때문에,본 논문에서는 공인 취약점 ID에 기반한 호환성 분석 방법을 사용하기로 한다.그러나 점검 결과로 발견된 취약점의 상당 부분이 공인 취약점 ID가 없다는 사실을 고려하여, 본 시스템에서는 공인된 취약점ID를 기본적인 식별 방법으로 사용하고, 공인 ID가 없는 취약점에 대해서는 No-match ID를 부여하고 그 특징을 기록 관리하는 방법을 사용한다. 이를 통해 서로 다른 취약점 점검 도구의 점검 결과간의 연관성 분석과 과거 점검 결과를 이용한 히스토리 분석을 수행할 수 있다.

본 논문에서는 다양한 취약점 점검 도구를 통합할 수 있는 자동화된 네트워크 취약점 진단 시스템을 설계하고, 점검 도구 통합시 발생할 수 있는 주요 문제점과 해결방안을 제시하였다.이 시스템은 다양한 점검 도구를 상호 보완적인 목적으로 사용하여 취약점 점검 결과의 정확성과 포괄성을 향상시킬 수 있다는 것이 가장 큰 특징이다. 또한 다양한 취약점 점검 도구를 쉽게 통합하여 사용할 수 있기 때문에 조직의 네트워크 환경과 재정적인 상황에 맞는 점검 도구를 선택할 수 있다는 장점이 있다.취약점 점검 결과와 점검 정책에 대한 히스토리 관리 기능을 통해 네트워크에 대한 종합적이고 지속적이며 일관성 있는 취약점 관리가 가능하다.