독립 실행 기반 가상자원 보안 점검 자동화 시스템에 관한 연구

김희재, 송현석, 이준영
한전KDN 전력ICT기술원 전력보안기술부
{hola.halo2, hyunseok.song.17, ljy.953386}@kdn.com

A Study on Automated Security Inspection Systems for Virtual Resources Using Independent Execution Environments

Hee-Jae Kim, Hyun-Seok Song and Jun-Young Lee
KEPCO-KDN. Power ICT Technology Institute, Power Security R&D Team

요 약

본 논문은 여러 가상 머신 자원의 독립적인 복제를 기반으로 가상 환경을 위한 자동화된 보안 점검 시스템을 제안한다. 외부 장치로부터 원본 정보를 수집하고, 미리 정해진 복제 시스템을 사용하여 독립적인 가상 머신 인스턴스를 생성하며, 독립된 환경에서 보안 평가를 수행한다. 분석 후, 시스템은 자동으로 보고서를 생성 및 전송하며 테스트 환경을 삭제한다. 이를 통해 신뢰할 수 있는 취약점 관리와 확장을 가능하게 하여 기존 한계를 극복하고 효율과 보안성을 향상시킬 수 있다.

Ⅰ. 서 론

기관 및 기업의 시스템 인프라는 유연성과 확장성이 갖춰진 가상화 기반 운영 환경으로 빠르게 전환되고 있어 시스템의 복잡성과 연결 지점이 증가함에 따라, 보안 취약점의 발견과 대응이 더욱 중요해지고 있다.[1]

기존 보안 점검은 수동 방식에 의존하며, 운영 중인 시스템과 점검 환경이 분리된 경우가 드물어 실시간 대응에 한계가 존재한다. 본 연구에서는 운영 안전성 및 자원 효율성을 확보하며, 점검을 빠르고 정확하게 할 수 있는 보안 점검 자동화 방법을 제안한다. 본 시스템은 복수의 외부 장치로부터 정보를 수집하여 독립된 가상 환경을 자동 복제하여 점검을 수행하고, 결과를 보고한 뒤 자원을 자동으로 회수한다.

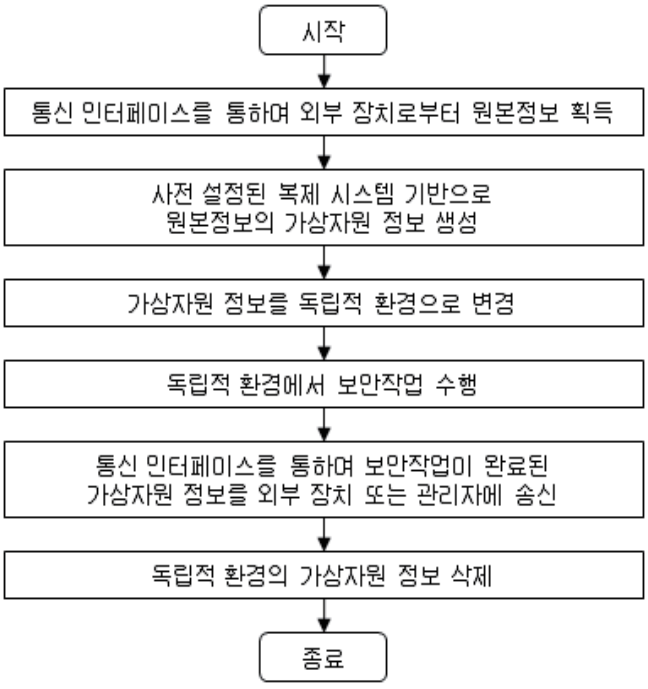
Ⅱ. 본론

2.1 기존 보안 점검 방식의 한계

기존 가상화 기반 인프라에서는 가상머신의 생성 및 배포는 자동화되었지만, 보안 점검과 테스트 환경 정리에 있어 자동화가 미흡한 한계가 있었다. 특히 운영 환경과 점검 환경이 물리적으로 분리되지 않은 구조에서는, 점검 중 실시간 서비스의 중단 가능성이나 민감 정보의 유출 위험이 지속적으로 제기되어 왔다.[2] 또한 수동으로 진행되는 점검 절차는 작업자마다 결과 편차가 크고, 처리 시간 증가 및 인력 소모로 이어진다. 점검 완료 후에도 점검 중 생성된 가상 실행 환경이 자동으로 폐기되지 않으면, 불필요한 시스템자원 점유와 보안 취약 요소의 잔존이 발생하며, 이는 전체 시스템의 신뢰도와 운영 효율성 저하로 연결된다.

2.2 제안하는 자동화 시스템

본 시스템은 복수의 외부 전자 장치로부터 수집한 보안, 시스템, 디스크, 메모리 정보 등을 기반으로 복제 시스템을 통해 복제 가상 환경을 자동으로 생성한다. 복제 방식은 스냅샷, 이미지 기반 생성, 라이브 마이그레이션 등 다양한 형태를 지원한다. 생성된 가상 환경은 원본과 완전히 분리된 독립의 환경으로 전환된다. 독립 환경에서 실시간 보안 점검이 가능하며, 점검 과정에서 운영 중인 시스템에 영향을 미치지 않아, 안정성과 보안성을 확보할 수 있다. 이러한 환경 구성을 통하여 보안 점검을 위한 테스트 환경의 독립성과 안정성을 보장하고, 자동화된 대응 체계 기반을 형성하고자 한다. 아래 [그림 1]에 시스템 서버가 동작하는 방법의 흐름도를 표현하였다.[3][4]



[그림 1] 제안 시스템의 서버 동작 방법 흐름도

2.3 자동화된 보안 점검 프로세스 제안

제안 시스템은 독립의 복제된 가상 환경에서 보안 점검을 자동화하여 수행한다. 아래 [표 1]과 같은 예시 항목 기준으로 자동화된 스크립트가 점검을 수행한다.

No.	내용
1	관리자 계정 활성화 및 게스트 계정 비활성화
2	패스워드 정책 준수 여부 (복잡도, 변경 주기 등)
3	포트 및 서비스 상태 확인 (불필요 서비스 비활성화 포함)
4	공유 폴더, 외부 연결 권한 설정
5	데이터베이스 서비스 접근 및 인증 설정

[표 1] 일반적인 점검 수행 기준 항목의 예시

이러한 항목들은 각 기관이나 기업의 보안 정책에 따라 커스터마이징이 가능하며, 정해진 기준에 따라 반복적이고 정확하게 점검할 수 있다.

점검 완료 후 시스템은 취약점 목록, 영향도 평가, 수정 권고사항 등이 포함된 보고서를 자동 생성한다. 보고서는 관리자에게 실시간으로 전송되며, 외부 감사기관에 제출 가능한 표준 형식으로도 출력될 수 있다.

점검 이후, 해당 테스트 환경은 자동으로 삭제된다. 이는 정보 유출 가능성을 줄이고, 불필요한 자원 사용을 방지함으로써 보안성과 운영 효율성을 동시에 확보하는 핵심 요소이다.

2.4 점검 시간 예측 모델 제안

점검 시간 예측 모델을 통하여 전체 작업 소요 시간(T_{total}) 산출 방법을 제안 하고자 한다.

독립의 복제된 가상 환경에서 점검이 이루어지기 전, 복제 소요되는 시간(T_g) 수식은 다음과 같다.

$$T_g = T_c + T_p$$

T_c : 원본 환경 캡처에 걸리는 시간 (ex. 10초)

T_p : 복제 환경 생성에 걸리는 처리 시간 (ex. 77초)

T_g : 복제 전체에 소요되는 시간 (ex. 평균 87초)

실제 시스템의 전체 작업 소요 시간(T_{total})은 복제 시간(T_g)과 점검 시간($N_{vm} \times T_{chk}$) 합으로 정의한다.

$$T_{total} = T_g + (N_{vm} \times T_{chk})$$

N_{vm} : 점검 대상 가상머신의 수

T_{chk} : 단일 가상머신 소요 점검 평균 시간 (ex. 46초)

*복수의 총 가상 머신 수와 소요시간은 비례하다.

**ex. 10개의 가상머신을 점검할 경우

$$T_{total} = 87 + (10 \times 46) = 547초$$

T_{total} : 전체 작업 소요 시간

이와 같은 모델은 점검 대상 수 증가에 따른 자원 소요를 예측하고, 병렬 처리나 스케줄링 전략 수립 시 활용될 수 있으며, 실시간 보안 진단을 위해 필요한 리소스를 사전에 확보하는 데 유용하다.

2.5 기술 비교 분석

제안 시스템은 기존 수동 점검 방식 대비 다음과 같은 기술적 차별성을 가진다. 첫째, 점검 환경의 완전한 격리를 통해 운영 환경에 영향을 주지 않으며, 둘째, 복제-점검-보고-삭제 전 과정을 자동화하여 인력 비용과 오류 가능성을 줄인다. 셋째, 점검 후 테스트 환경을 자동으로 삭제함으로써 자원 낭비를 방지하고, 마지막으로 실시간 보고 기능을 통해 보안 관제 및 감사 대응력을 강화할 수 있다.

이러한 장점은 병렬 점검을 통해 수십에서 수백 대의 가상머신에 대한 동시 보안 진단을 가능케 하며, 특히 금융, 전력, 공공기관과 같이 높은 보안 신뢰성이 요구되는 환경에서의 활용을 기대해볼 수 있다.

Ⅲ. 결론

본 연구에서는 복수의 외부 전자 장치로부터 수집한 정보를 기반으로 가상 환경을 자동 복제하고, 독립된 환경에서 보안 점검을 수행하며, 결과를 실시간 보고하고 점검 환경을 자동으로 삭제하는 통합 시스템을 제안하였다. 해당 시스템은 운영 환경과 분리된 구조에서 실시간 점검이 가능하고, 자동화된 보고 및 자원 회수 기능을 통해 보안성과 운영 효율성을 동시에 향상시킨다. 특히 병렬 점검 구조를 통해 대규모 가상 환경에서도 높은 확장성과 신뢰성을 제공하며, 기존 수동 방식 대비 보안 관리의 정밀성과 대응 속도의 개선을 기대할 수 있다.

향후에는 다양한 원격 컴퓨팅 서비스 환경 간 상호 운용성 강화, 양자암호 기반 통신 적용 등으로 기술 고도화함으로써, 지능형 가상 환경 보안 플랫폼으로 발전시킬 수 있다. 이러한 기술고도화는 가상 환경의 복잡성과 보안 위협에 대응할 수 있는 보안 관리체계를 마련하는 데 기여할 것이다.

참 고 문 헌

[1] 한국지능정보사회진흥원(NIA), “클라우드 컴퓨팅 동향-2025 플렉세라 보고서 분석,” 디지털서비스 이슈리포트 2025-03호, 2025..

[2] 김환국, 조화, 신영상. 안전한 클라우드 환경구축을 위한 가상화 보안 이슈 및 기술 동향. 한국통신학회지(정보와통신), 32(10), 49-57, 2015.

[3] Tsifountidis, Fotis. "Virtualization security: Virtual machine monitoring and introspection." Signature 49, 2010.

[4] RedHat, “Managing virtual machines and containers,” Technical Whitepaper, 2022.