

초연결네트워크

공격그래프 기반 자동화된 보안성 평가 기술

- 특허명 : 네트워크 보안 강화 장치 및 그 방법 (10-2017-0101671)
- 보유기관 : 한국전자통신연구원
- 상태정보 : 출원 '17.08.10 > 공개 '19.02.20
- 기타정보 : 관련특허 포트폴리오 구축(총 2건)



기술개요

- 조직 내의 ICT 장비들과 설치된 OS, SW 정보, 취약점(CVE)정보를 자동 수집 및 분석 기술
- ICT 자산 정보에 기반한 대상 도메인의 네트워크 토폴로지 자동 생성 및 관리 기술
- 공격 그래프 기반 공격 경로 예측 및 보안성 평가 기술
- 보안성 점검을 자동으로 해주는 BAS(Breach and Attack Simulation)솔루션에 적용 가능함

기존 문제점

- ICT 자산정보 수집 기술은 네트워크 스캐닝을 통한 자산정보 리스트만 제공, 자동화된 국내 기술은 없음
- 보안성 평가는 모의해킹 등 사람에 의한 수동적으로 진행

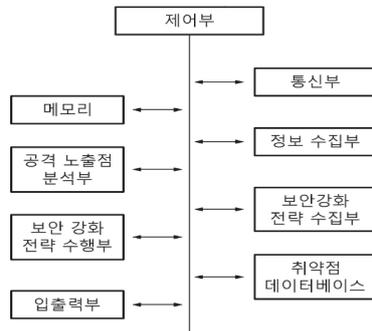


기술 차별점

- ICT 자산정보의 자동 수집 및 분석을 통해 대상 도메인의 네트워크 구조를 관리
- ICT 자산정보 및 취약점 정보를 확률적으로 계산된 공격 경로 자동 예측

세부내용

- IT자산 정보, 네트워크 토폴로지 정보, CVE 취약점 DB 정보를 자동수집하고 분석하여, 공격에 사용될 수 있는 가능성이 높은 공격 경로를 예측하고 시뮬레이션 및 가시화하는 기술
- 네트워크 상의 호스트들의 공격 노출점을 분석하고 보안을 강화할 부분을 식별하여 해당 호스트에 대한 보안 강화를 실행함



- 한국전자통신연구원 김호민(042-860-1804, hominkim@etri.re.kr)
- 공동마케팅사무국 서원우(042-862-6018, sww93@wips.co.kr)