Line up

제품	구분	상세 분류	
SECUI SCAN V3.1	3 Tier / Stand Alone	SECUI SCAN v3.1 UNLIMITED	모든 IP 대역에 대해 점검할 수 있는 버전 점검 가능 IP 대역 : 예) 1.1.1.1 ~ 255.255.255.254 용도 : 보안 관련 컨설팅 업체 진단/컨설팅 및 대규모 네트워크 관리
		SECUI SCAN v3.1 A CLASS	A Class : 지정된 IP Class A 대역에 대해 점검할 수 있는 버전 점검 가능 IP 대역 : 예) x.1.1.1 ~ x.255.255.254 용도 : 대규모 사업장에서 사용
		SECUI SCAN v3.1 B CLASS	B Class : 지정된 IP Class B 대역에 대해 점검할 수 있는 버전 점검 가능 IP 대역 : 예) x.x.1.1 ~ x.x.255.254 용도 : 중대형 규모의 사업장에서 사용
		SECUI SCAN v3.1 C CLASS	C Class : 지정된 IP Class C 대역에 대해 점검할 수 있는 버전 점검 가능 IP 대역 : 예) x.x.x.1 ~ x.x.x.254
		* 3 Tier 형식은 추가 Agent 구매 가능	

점검 영역

Applications (Web, DB)

- HTML 5, AJAX(XML 1.1) 취약점 점검
- 웹 서버 점검
  - IIS, Apache 등의 웹 서버 취약점, 설정 점검
  - RDS, Unicode 등의 취약점 정밀 점검
  - 각종 CGI 취약점 점검
  - Deep Scan 기능 : 웹 미러링 기술을 통한 Unknown 취약점 점검(SQL Injection 등) Depth Level (Default 5 Level)
- 웹 Proxy 서버 취약점 점검
- 데이터베이스 점검
  - Oracle, MS SQL, MySQL 서버 취약점 점검
  - 각종 디폴트 패스워드 점검

UNIX / Linux Systems

- SSH 로그인을 통한 Local Security 점검
- Backdoor 점검 : Trinoo, mstream 등
- SMTP 버전 및 취약점 점검
- rsh, rlogin, rexec, telnet 점검 : Brute force attack
- SNMP 취약점 점검 : community name, read/write
- FTP/TFTP 서버 취약점 점검
- DNS 서버 점검 : bind
- RPC 서버 점검
- NFS 공유, NIS 점검
- X-window remote 취약점 점검
- 불필요한 서비스 점검 : Echo, Time, Chargen 등
- 위험 서비스 점검 : Finger, Gopher, POP3, SSH 등

Windows Systems

- Backdoor 점검 : Back Orifice, CDK 등
- Remote Control Program 점검 : NetBus 등
- NetBIOS 서비스 취약점 점검
  - 사용자 목록 획득을 통한 로그인 시도
  - 공유 폴더 버그, 공유 권한 등 점검
  - Remote Registry 점검 : AutoLogon 등
- SNMP 취약점 점검 : community name, read / write
- FTP 취약점 점검 : Anonymous, guest
- UNIX 계열 서비스 점검 : X-window, TFTP 등
- 불필요한 서비스 점검 : Echo, Time, Chargen 등

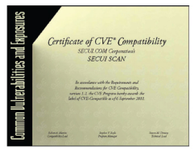
Network Equipment

- 보안 상태 점검 : 통신 장비 (Router, Switching Hub, F/W, IDS 등)
- SNMP 취약점 점검 : community name, read/write
- TCP, ICMP 취약점 점검 : TimeStamp 등
- 각종 Stealth Port Scan에 의한 포트 스캔 테스트
- 디폴트 패스워드에 의한 Brute Force 공격 시도

CERTIFICATIONS >>



CC 인증



CVE - Compatible 인증

SECUI (주)시큐아이

서울특별시 중구 소공로 48 5~7F
tel 02 3783 6600 **fax** 02 3783 6499 **www.secui.com**

대표전화 080 331 6600
침해대응센터 02 3783 6500
평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)

Copyright® SECUI All Rights Reserved. 본 카탈로그에 게재된 회사명, 상품명은 당사의 등록 상표입니다.
사양과 외관은 개량을 위해 예고 없이 변경되는 경우가 있습니다.

SECUI

SECUI SCAN v3.1

국내 최초 통합형 취약점 점검 솔루션

SECUI

SECUI SCAN

SECUI SCAN은
시스템 및 네트워크 장비와 보안장비의 다양한
보안 취약점과 웹 취약점을 점검하는
Scanner 솔루션입니다.

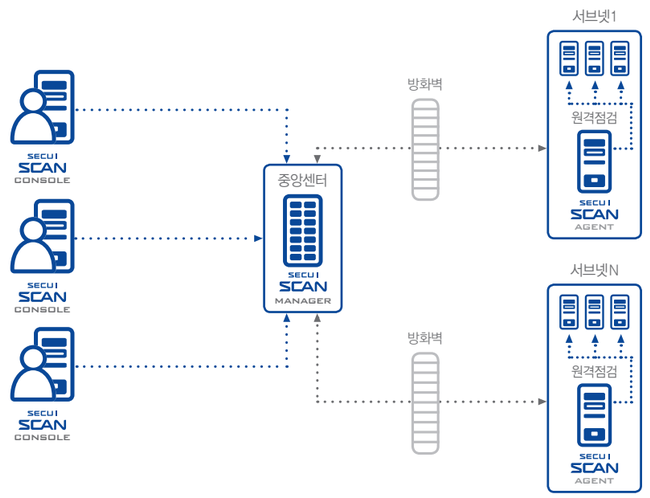


Key Features

- 중앙관제형 (3 Tier 방식) 통합형 스캐너 (네트워크+웹+개인정보 탐지)
- 다중의 사용자 동시 점검 지원
- 고성능 URL 수집 기능 및 웹 HTML 5, AJAX(XML 1.1) 취약점 점검 기능
- 알려진 국산 게시판 취약점 점검
- 국정원 8대 보안 취약점 점검
- OWASP 10대 보안 취약점 점검

중앙관제형 (3 Tier)의 취약점 점검 툴 구성으로 중앙의 관제센터에서 관리 대상 서브넷들을 통합 관리
(Stand Alone 형태로도 구성 및 운영이 가능)

– 콘솔 (Console) : 사용자 User Interface
– 매니저 (Manager) : 중앙관제센터에 설치되며, 에이전트들의 점검 결과를 통합 관리
– 에이전트 (Agent) : 실제 점검 기능을 갖추고 있는 스캐닝 엔진을 탑재한 서비스 프로그램



Key Specifications

취약점 점검

콘솔 Console

- 점검 작업의 실시간 모니터링 및 작업의 원격 통제
- MS Windows 기반의 UI 프로그램 (플랫폼 : MS Windows 7 SP1 이상)

매니저 Manager

- 중앙에서 콘솔과 에이전트로부터 발생하는 작업을 처리하는 역할
- MS Windows 기반의 서비스 프로그램
  (플랫폼 : MS Windows 7 SP1 이상, 메모리 2GB, CPU Dual Core 2.6 Ghz 이상)
- Microsoft SQL Server 2014 Express 사용, MS SQL 연동 가능

에이전트 Agent

- 점검 엔진을 구동시켜 실제로 점검 작업을 수행하는 프로그램
- MS Windows 기반의 서비스 프로그램
  (플랫폼 : MS Windows 7 SP1 이상, 메모리 2GB, CPU Dual Core 2.6 Ghz 이상)
- Microsoft SQL Server 2014 Express 사용, MS SQL 연동 가능

Key Functions

다양한 취약점 스캐닝

- Windows, Linux, Unix 등의 일반 운영체제를 비롯해 각종 네트워크 장비, 보안 장비에 대한 광범위한 점검 기능
- 다양한 네트워크 프로토콜의 취약점 점검
- 서비스 거부 (DoS) 취약점에 대한 점검 정책 별도 분리

웹 서버 점검 기능

- HTML 5, AJAX(XML 1.1) 취약점 점검 기능
- 웹 서버 자체의 알려진 취약점 점검 기능
- JavaScript 처리 엔진과 Flash 파일 처리기를 내장하여 강력한 Crawling 기능 제공
- 각종 웹 패키지 소프트웨어 (ZeroBoard, PHP-Nuke, PostNuke 등) 알려진 취약점 점검 기능
- 웹 애플리케이션상의 각종 취약점 (SQL injection, XSS, File Upload 등) 점검 기능
- 숨겨진 웹 폴더 추측 점검 기능
- 각종 인증 (Form 로그인 인증, 디렉토리 기반 인증) 기반의 인증 세션 유지 점검 기능
- 웹상에 유출된 개인정보 (주민등록번호, 전화번호, 신용카드 정보, 사용자 정의 패턴 등) 탐지 기능

개인정보 탐지 기능

- 최근 문제가 되는 개인정보 (주민등록번호, E-mail, 신용카드 번호, 전화번호)가 포함된 웹 페이지 검색/리포팅
- 사용자 정의 정규 표현식 점검 패턴 기능

중앙관제형 스캐너

- 스캐너의 중앙관제 : 중앙관제형 스캐너를 통해 분산된 네트워크의 통합 점검 작업 지원
- 다중의 사용자 지원 : 사용자별 별도의 점검 권한 및 점검대역 부여
- 다중 세션 제공 : 한 사용자가 각기 다른 정책을 가진 여러 점검 작업의 동시 수행 지원
- 다중 에이전트를 이용한 병렬 점검 : 분산된 네트워크에 각각 설치된 에이전트를 통한 병렬 점검 수행