보안취약성 분석! 무엇으로 하시겠습니까?

Secuguard NSE

보안의 첫 걸음!
Secuguard NSE로 점검하십시오!

국내기술로 개발된 네트워크 취약점 점검도구 NSE는 네트워크에 연결된 모든 시스템들의 다양한 보안 취약점들에 대해서 자동으로 진단하고 발견된 문제들에 대한해결 방법을 제공하여 해킹과 컴퓨터 범죄들로부터 보호하고 예방할 수 있는 보안 소프트웨어 솔루션입니다.

국내 최초의 CVE
인증마크 획득
CVE(Common Vulnerability Exposure)

CC인증획득
CC인증 EAL2등급 획득
CC(Common Criteria)

NSE 상세 특징

✓ 국내 최초로 CEV Compatibility 인증 획득
- 국제 보안취약점 표준화 단체 MITRE로 부터 보안취약점 표준을 준수하는 제품에만 인증하는 CVE(Common Vulnerability Exposure) 인증 획득

✓ 편리한 사용자 인터페이스
- 직관적이고 한글화된 사용자 인터페이스
- 모든 기능에 대해 친절하고 자세한 온라인 도움말 제공
- 서버별 점검이력, 진행사항, 점검결과 화면과 이해하기 쉬운 보고서

✓ 빠르고 강력한 보안취약점 점검
- 일괄점검, Agent별 점검, 항목별 점검등 다양한 점검방법 제공
- 동시에 모든 점검 대상에 대한 점검을 수행
- 발견된 보안취약점의 위험수준, 내용, 영향 및 조치방안을 제시
- Knowledge Base를 이용하여 점검 모듈간 정보공유로 점검시간 대폭 단축

✓ 점검대상 시스템 및 운영체제 자동인식 기능
- Network 자동탐색
- 운영체제 종류 자동 판별
- DNS명 판독
- 윈도우 운영체제인 경우 네트워크 노드명 판독

✓ 상세한 취약점 정보 제공
- 취약점 데이터베이스를 기반으로 다양한 형태의 취약점 정보 제공
- 취약점 그룹별, 운영체제별, 위험도별 취약점 정보 제공

✓ 온라인 및 오프라인 자동 업데이트
- 콘솔 모듈 자동 패치
- 최근의 보안취약점 점검모듈을 인터넷을 통해 자동 업데이트

✓ 통신 및 자료의 암호화 처리로 보안 강화
- 콘솔과 서버 간의 통신 메시지를 암호화 처리하여 내용이 유출되어도 안전
- 모든 취약점 점검 결과는 암호화 처리하여 파일에 저장
- 인증된 콘솔과 사용자만이 취약점 점검 실행 및 내용 조회 가능

✓ 보안 관리의 중앙 집중화
- 하나의 콘솔 / 에이전트에서 분산된 여러 서버에 대한 보안 취약점 점검을 동시에 수행
- 여러 대의 호스트에 대하여 동시에 보안취약점 점검을 수행하므로 점검시간 대폭 단축

✓ 다양한 보고서 및 부가 기능
- 취약점 목록보고서, 위험도별 취약점 분포 보고서 등 14종 이상의 다양한 보고서
- Crystal Report를 이용하여 작성된 다양한 그래프 및 표 형태 보고서
- HTML, Word, Excel 및 PDF 등 다양한 파일형식으로의 보고서 변환기능 제공
- 보고서 제외취약점 설정기능
- 그룹별 Agent 관리기능

✓ 간편한 설치와 손쉬운 확장
- 하나의 콘솔에 서버와 에이전트 설치로 간편
- 부하 분산을 위해 다중 콘솔 운영 가능

NSE 기대 효과

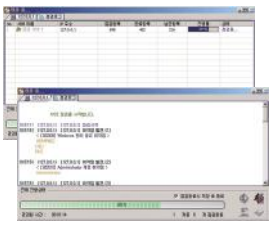
보안사고 예방활동에 필요
주기적으로 운영중인 정보시스템의 보안 취약점 분석을 통하여 사고를 예방하기 위한 활동을 할 수 있습니다.

보안수준 향상을 기대
수많은 보안취약점을 취약점 분석도구를 통해 이해할 수 있으며, 이를 관리 정책 등에 반영하여 보안 수준 향상을 기대 할 수 있습니다.

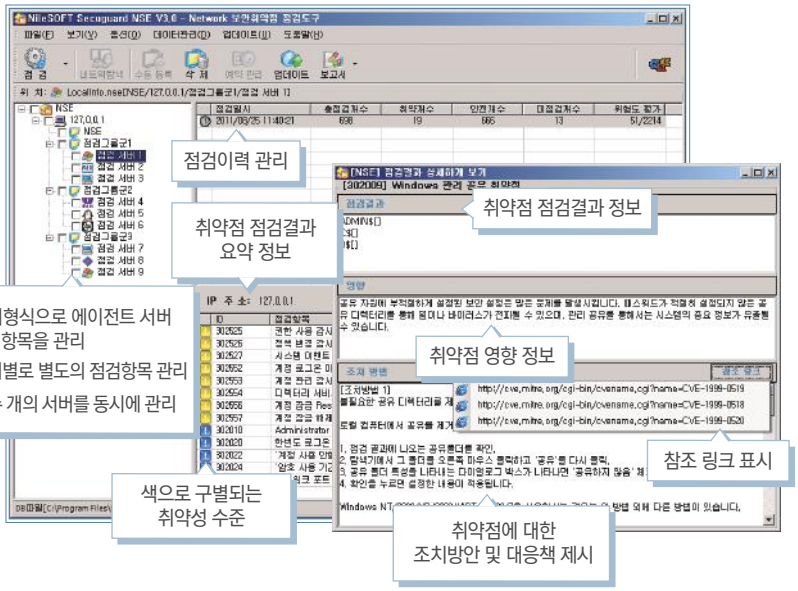
보안수준 평가 도구
원하는 시점에서 현재 정보시스템의 보안상태를 파악 할 수 있으며 이를 기반으로 정보시스템의 안전한 운영을 도모 할 수 있습니다.

재해(안전) 대책
평소 보안 취약점 분석 및 조치를 통하여 침입차단, 침입 탐지 시스템의 장애 시 피해를 최소화 할 수 있습니다.

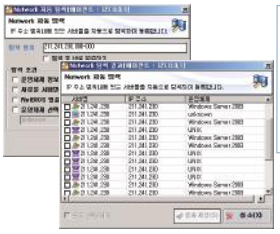
NSE 실행화면 및 기능



▲ 점검진행화면

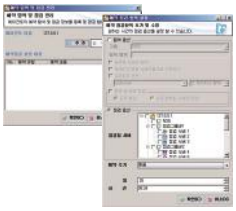


▲ 점검항목 편집 기능



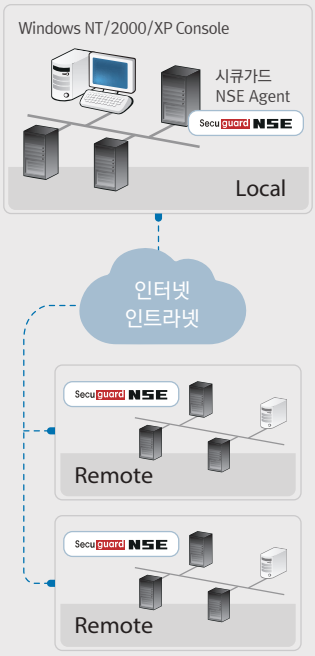
- 트리형식으로 에이전트 서버 점검항목을 관리
- 서버별로 별도의 점검항목 관리
- 복수 개의 서버를 동시에 관리

▲ 네트워크 탐색화면



▲ 항목별 점검 및 예약점검 기능

NSE 구조도 및 점검항목



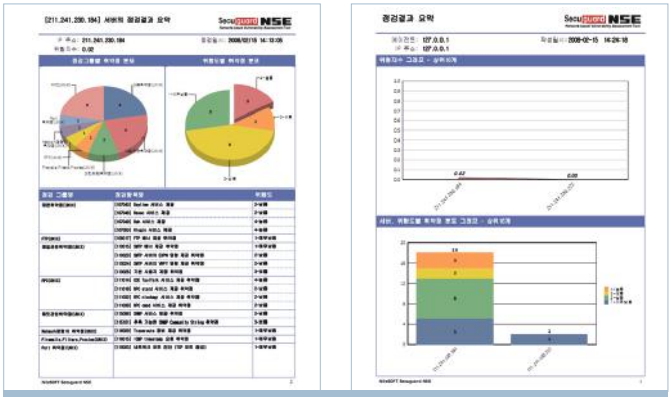
UNIX/Linux 계열 점검항목

- X Windows 관련 취약점
- 관리자 및 사용자 환경 취약점
- Utilities 취약점
- File Systems 취약점
- Databases 취약점
- Daemons 취약점
- Backdoors 취약점
- NIS/NIS+ 취약점
- Port 취약점
- SMTP and Mail 관련 취약점
- Remote Procedure Call 취약점
- WWW/HTTP와 CGI 취약점
- DNS/BIND 관련 취약점
- 원격접속 명령어 취약점
- Packets 관련 취약점
- Network Commands 취약점
- Firewalls/Filters/Proxies 취약점
- File Transfer Protocol(FTP)취약점

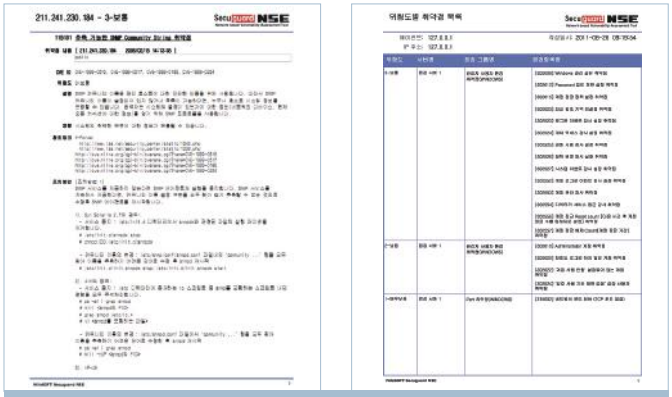
Windows 계열 점검항목

- Password 관련 취약점
- 관리자 및 사용자환경 취약점
- 기타 서버 서비스 취약점
- File Systems 취약점
- Databases 취약점
- 특정 파일 취약점
- Port 취약점
- Internet Explorer 취약점
- Internet Information Server 취약점
- Server Services 취약점
- 응용 프로그램 취약점
- 기타 응용 프로그램 취약점
- Exchange Servers 취약점
- Registry 취약점
- WWW/HTTP와 CGI 취약점
- Packets 관련 취약점
- Firewalls/Filters/Proxies 취약점
- SMTP와 Mail 관련 취약점
- Backdoors 취약점

NSE 다양한 보고서



▲ 요약 보고서



▲ 상세 보고서

NileSOFT
서울시 구로구 구로동 디지털로 32길 30, 코오롱디지털타워 빌란트1차 1004호
TEL. 02-783-0961 FAX. 02-783-0963 e-mail. nileman@nilesoft.co.kr
www.nilesoft.co.kr
정보보호의 대중화! 나일소프트가 함께 하겠습니다