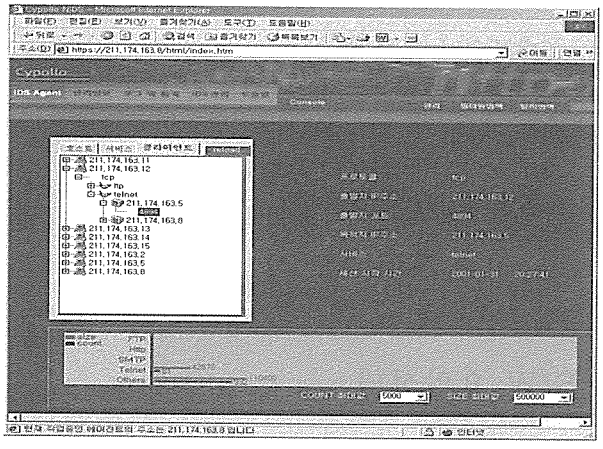
조은시큐리티 'Cypollo'

네트워크 침입탐지 시스템
완벽한 정보보호 시스템

조은시큐리티(대표 최성백)의 Cypollo는 국내 독자 기술로 개발된 침입탐지시스템이다.



조은시큐리티 싸이폴로(Cypollo)

네트워크 기반과 호스트 기반의 제품 2종류가 있으며 외부 침입자가 컴퓨터 시스템이나 네트워크의 자원을 권한 없이 불법적으로 사용하기 위한 시도 또는 내부 사용자가 자신의 권한을 오·남용하여 권한 외의 자원을 사용하기 위한 시도를 탐지하여 그 피해를 최소화하는 시스템이다.

이 제품의 기능으로는 ▶실시간 침입탐지 및 위험요소와 대응방안 제시 ▶불법행위에 대한 세션 차단 ▶의심스러운 특정 사용자 모니터링 및 세션 강제 종료 ▶로그분석을 통한 Playback 기능 ▶시스템 자체 무결성 검사 ▶다양한 통계출력 및 보고서 작성 등이 있으며, ▶강력한 사용자 인증(One Time Password) ▶등급별 관리자 권한 부여 ▶사용자 네트워크 환경에 최적화 할 수 있도록 다양한 환경설정 지원 ▶Sniffing 방지(Secure Socket Layer 사용) ▶분산환경에 의한 뛰어난 확장성 및 대규모 네트워크 지원 등의 장점을 갖는다. Cypollo는 외부 인터페이스를 통한 침입탐지 후 대응 및 보안관제센터에서 통합관리가 용이하며 회사 자체에서 운영하고 있는 해킹분석 및 대응팀에서 최신 해킹기법에 대한 신속한 Ruleset Upgrade를 하고 있는 것도 장점이라 할 수 있다.

Cypollo-nv1.1

장 려 상

1. 작품명 : Cypollo (침입탐지시스템)

2. 제작자 : (주) 조은시큐리티

대표자 : 최성백

개발참여자 : 한재호, 안석순, 김준남, 황상구

서경대학교 컴퓨터공학과 이양선 교수

주소 : (135-931) 서울시 강남구 역삼동 811 성우빌딩 2층

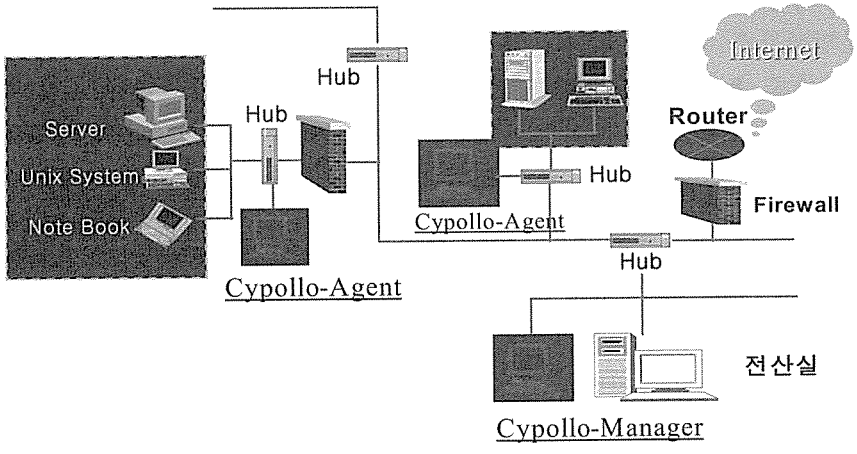
전화 : 02) 556-7970

팩스 : 02) 556-7971

email : support@joeunsecurity.com

3. S/W 요약설명

네트워크 침입탐지 시스템은 사용자 및 외부 침입자가 컴퓨터 시스템이나 네트워크의 자원을 권한 없이 불법적으로 사용하기 위한 시도 또는 내부 사용자가 자신의 권한을 오·남용하여 권한 이외의 자용을 사용하기 위한 시도를 탐지하여 그 피해를 미연에 방지하고 최소화하는 시스템이다.



3.1 개발 배경

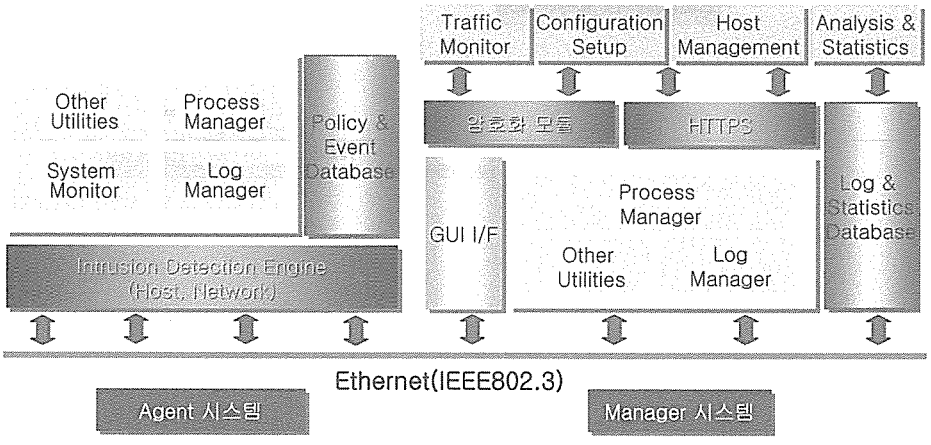
지속적인 해킹수법의 출현과 다양한 유형 때문에 정보통신망 및 정보시스템 운영기관에서의 효과적인 대응이 점점 어려워지고 있다. 본 제품 Cypollo는 실시간으로 침입을 분석하고 탐지하여 관리자에게 자동으로 보고하며, 대규모 네트워크에서도 효율적으로 관리를 할 수 있도록 지원하는 분산형 침입탐지 시스템이다.

3.2 시스템 개요

네트워크 침입탐지 시스템 Cypollo의 구성은 침입탐지 엔진, Data Base, 사용자 인터페이스의 3부분으로 나뉘어지며 Data Base와 Application은 분리하여 DB의 Load를 최소화할 수 있는 구조이다.

사용자 인터페이스는 Web 환경에서 운용되며 주로 DB와 연동되어 처리되며 필요한 경우 TCP/IP Socket을 통해 데이터를 주고받는다.

Application은 DB와 독립적으로 Memory에서 Data를 참조하게 되어 DB에 문제가 발생하였을 경우에도 운용이 가능하도록 설계되어 있다.

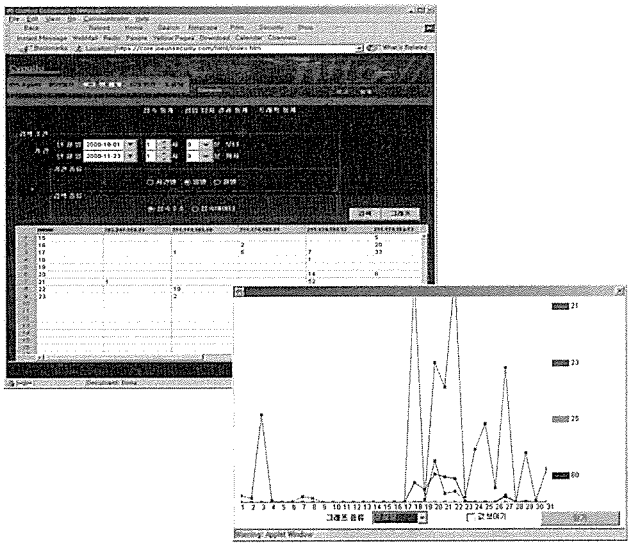


< Cypollo Architecture>

3.3 시스템 주요기능

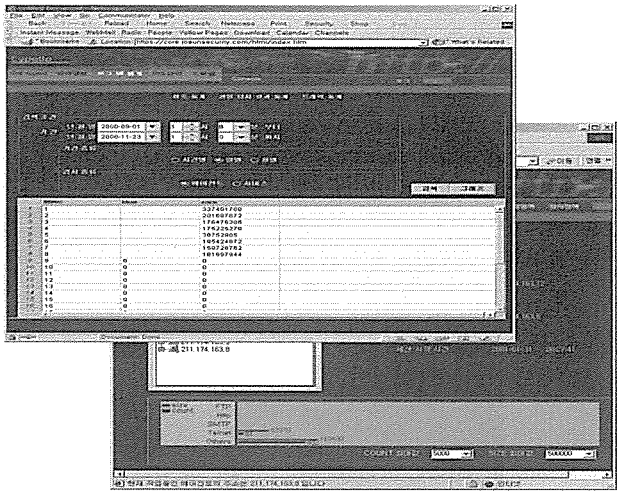
◉ 다양한 통계 출력 및 보고서 작성

로그검색을 통해 침입탐지 결과, 관리자 접속 등에 대한 로그를 조건별로 검색하여 원하는 결과만 볼 수 있고 침입탐지, 트래픽, 접속 통계를 검사기간과 종류별로 통계를 볼 수 있으며 그래프로 출력하여 보다 편리하게 보고서를 작성할 수 있다.



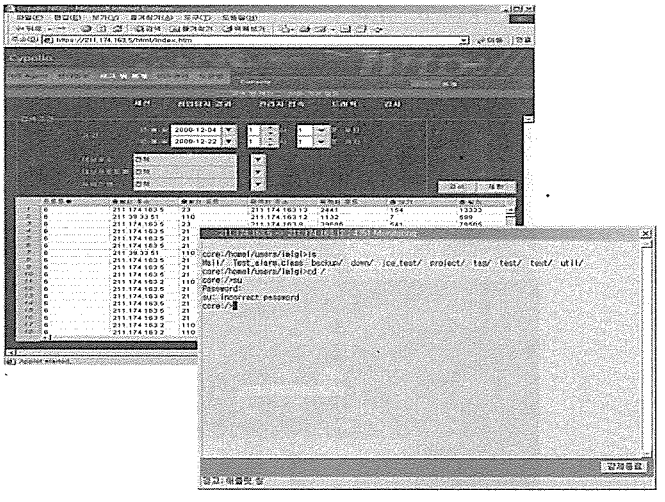
◉ 네트워크 트래픽 사용에 대한 분석 및 통계

네트워크 서비스별(Telet, FTP, SMTP, HTTP, others)로 트래픽을 측정하여 실시간 그래프로 볼 수 있으며 트래픽 통계 분석을 통해 네트워크 부하 측정이 가능하다.



◉ 로그분석을 통한 Playback 기능

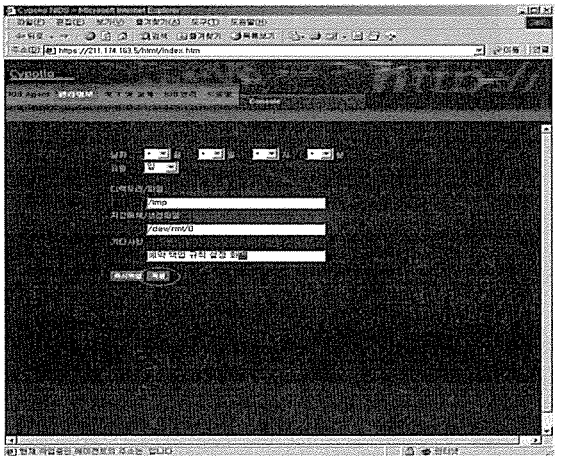
침입이 탐지된 정보를 가지고 세션로그를 검색하여 침입행위에 대한 재현(Playback)이 가능하므로 정확한 침입행위에 대한 분석이 이루어진다.



◉ 데이터 백업 예약 기능

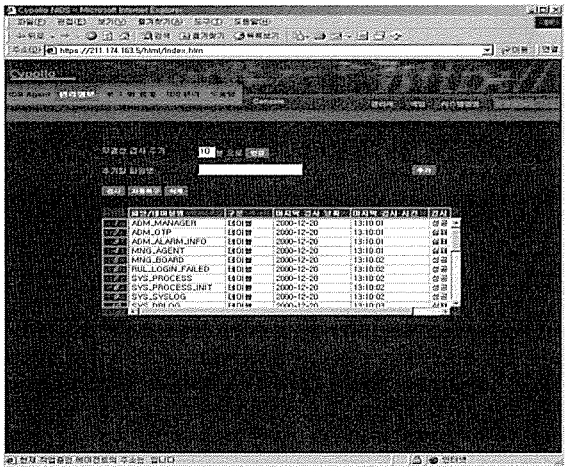
시스템 로그 및 감사기록에 대한 백업을 월, 일, 시, 분을 지정하여 예약할 수

있다. 또한 보통의 업무가 주단위로 이루어지므로 요일을 지정하여 예약할 수도 있다. 이렇게 예약을 하면 관리자가 별도로 백업을 하지 않아도 자동으로 백업이 이루어지므로 편리하게 시스템을 운영할 수 있다.



◉ 시스템 자체 무결성 기능

침입탐지시스템의 내부 데이터가 외부의 영향에 의해 자료가 변조되거나 임의로 변형이 가해진 상태를 점검하여 데이터 변조위협으로부터 안전하다. Cypollo의 무결성 검사는 시스템과 직접적인 관련이 있는 파일과 데이터베이스 테이블들에 대해서는 관리자가 지정해 놓은 시간간격마다 실행된다.



3.4 시스템 특징 및 장점

◉ **조직의 특성에 맞는 보안정책 수립**

사용자 환경에 맞는 Ruleset을 마음대로 추가 삭제가 가능하며 Cypollo Agent별로 별도의 Ruleset을 운영할 수도 있으므로 조직의 특성에 따라 보안정책수립이 용이하다.

◉ **H.A.R.T 운영**

Hacking Analysis & Response Team을 자체 운영하여 최신 해킹기법에 대한 분석 및 대응을 통해 신속한 Ruleset Upgrade지원.

◉ **분산환경에 의한 뛰어난 확장성 및 대규모 네트웍 통합관리**

Manager/Agent의 분산구조로 대규모 네트웍에도 적용하기 용이하도록 설계되어 있으므로 여러 대의 Agent가 설치되어도 통합관리가 가능하다.

◉ **Web Based IDS(SSL사용)**

웹을 기반으로 한 침입탐지시스템은 단순하고 개념적인 보안 서비스를 통해 보안 정책에 대해서 전문적인 지식이 부족한 일반 사용자도 쉽게 보안시스템 **운영 가능하다.**

◉ OTP

OTP(One Time Password)를 사용하여 패스워드의 노출 없이 안전한 로그인을 제공한다.

◉ **SNMP Trap**

망관리 프로토콜인 SNMP를 제공하여 보안관제센터 및 망관리 센터등과 연동되어 타 시스템과의 연동 및 집중관리를 용이하게 한다.

◉ **네트워크 상황에 맞는 최적의 시스템 설정**

프로토콜(TCP,UDP,ICMP …)과 서비스(telnet,ftp,e-mail.web …)도 사용자 정의에 의해 설정할 수 있으므로 사용자 네트워크 상황에 맞는 최적의 시스템 설정이 가능하다.

4. 개발단계별 기간 및 투입인원수

개발단계	개발기간	인원	공수	비 고
시스템 구상	99.10. 1~00. 1.31	4	8	KISA 기술이전 및 분석
시스템 설계	00. 1. 1~00. 4.30	5	29	기본설계 및 모듈별 상세설계
프로그래밍	00. 4. 1~00. 8.31	3	13	모듈별 프로그램 제작
시험 및 수정	00. 7. 1~00.10.31	5	20	모의 해킹 및 네트워크 부하 테스트
버전 Upgrade	00.11. 1~01. 4.30	5	70	설계 변경 및 보완
Linux Porting	01. 5. 1~01. 7.31	5	16	Linux System 구축
매뉴얼 제작	01. 7. 1~01. 7.31	5	5	패키지, CD디자인 및 매뉴얼 3종류 제작
계	22 개월		161	

5. 사용 또는 개발언어, TOOL

구분	프로그램명	비 고
Web Program	html	apache 1.3.17
	java	JSDK 1.3
	jsp	Jakarta Tomcat 3.1
Database	sql	MySQL 3.22.32
	jdbc	mm.mysql 2.0.4
System Program	c	egcs-2.91.66
	perl	Perl 5.005
Cipher Program	SSL	openssl 0.9.6
	modssl	modssl 2.8.0

6.사용시스템

	Agent	Manager	통합형 (Manager+Agent)
운 영 체 제	SuSE Linux 7.1k SUN Solaris 8	SuSE Linux 7.1k SUN Solaris 8	SuSE Linux 7.1k SUN Solaris 8
C P U	Intel PIII 500 이상	Intel PIII 500 이상	Intel PIII 800 이상
Memory	256MB 이상	128MB 이상	256MB 이상
HDD	8GB 이상	2GB 이상	10GB 이상
네트워크 인터페이스	NIC 1개이상	NIC 1개이상	NIC 1개이상
네트워크	Ethernet (IEEE802.3)	Ethernet (IEEE802.3)	Ethernet (IEEE802.3)