TESS

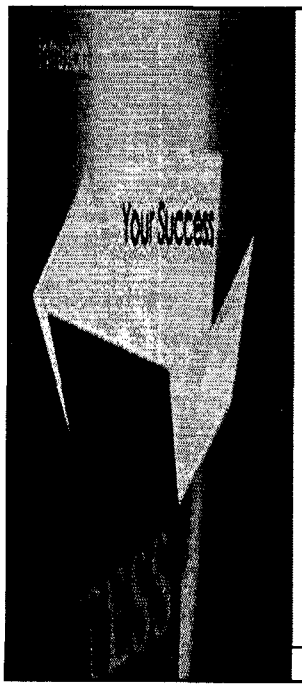
대학 네트워크 유해 트래픽으로 인한 피해 및 대응 방안

TESS NIDS
TESS IP-Wall
TESS HIDS
Threat Management System
Total Solution

2003년 5월 16일

INFOSEC
(주)정보보호기술

㈜위즈넷시스템즈



TESS

1. Overview
2. 제품주요기능
3. Reference

대학네트웍 침입탐지시스템 왜 도입하는가??

TESS

대학네트웍 보안의 한계성

- 대학의 네트웍은 유동적인 사용자들 때문에, 전체적으로 보안이 취약한 상태로, 보안정책에 따른 보안관리가 수행되고 있지 않음
  - ❖내부 네트워크와 인터넷의 구분이 명확치 않음.
  - ❖중요한 서버들과 일반 시스템들, 사용자 PC, 그리고 학생 시스템 및 단과대 시스템들이 모두 동등한 보안 수준을 가지고 있음.
- 불필요한 네트웍 서비스들이 많이 열려있으며, 이들 중 대부분은 취약점을 가지고 있어 빈번하게 공격에 이용되고 있음.
  - ❖많은 시스템들은 버퍼 오버플로우 공격을 통한 침입이 가능
  - ❖파일 정보를 읽어올 수 있는 시스템들도 발견
- 인증 및 접근통제 기능 미비
  - ❖몇 개의 서버에 대한 특정 서비스만을 부분적으로 제한하는 정도로만 되어 있어 실효성이 매우 적음
  - ❖이 중 어느 하나의 시스템만 점령하면 네트워크 전체를 손쉽게 장악
- 네트웍에 대한 감사 증적 또는 침입탐지 기능이 없음
  - ❖어떤 시스템이 불법 침입을 당해도 어디에서 어떻게 공격을 해왔는지는 물론 침입을 당한 사실조차 파악하기 쉽지 않음

대학네트웍 침입탐지시스템을 왜 도입하는가??

TESS

대학네트웍 보안의 한계성

- 스니핑을 통해 로그인 정보 등 전송되는 데이타를 모두 읽을 수 있음.
- 시스템에 대한 접근통제 기능이 구현되어 있지 않아, 라우터에서 외부로부터의 일부 접근을 통제하는 것 외에는 불법 침입을 막을 방법이 없음
- 네트웍 증설이 빈번히 이루어 지나 성능향상은 이루어지지 않고 있음.
  - ❖대부분의 대학 네트웍들의 80%이상이 불필요한 사용이나 이를 감지할 방법이 없음..
- 사용자들의 보안개념 취약. 보안시스템은 성능문제로 인하여 대학 전산망에서 사용할 수 없다고 단정

대학네트웍 침입탐지시스템을 왜 도입하는가??

TESS

네트웍보안의 한계성 해결!!

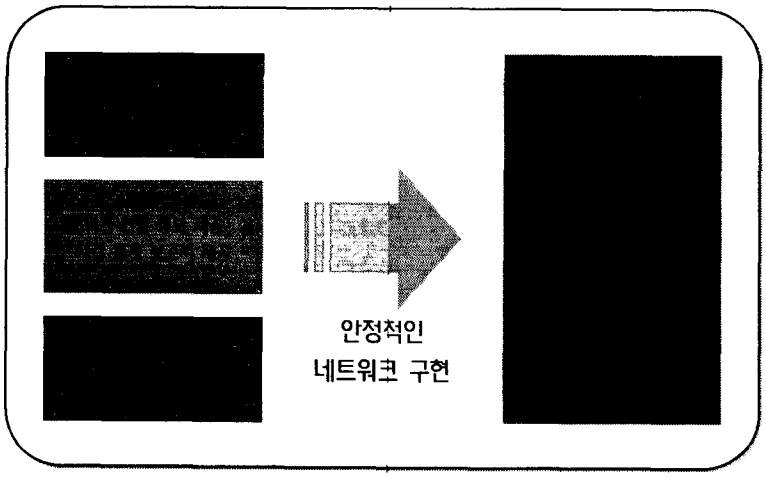
- ❑ 불필요한 네트웍 서비스들의 취약성 분석이 가능
  - ❖많은 시스템들 버퍼 오버플로우 공격탐지
  - ❖보안 정책이 없어, 마음대로 파일 정보를 읽어올 수 있는 시스템들을 찾아냄
- ❑ 전체 네트웍 사용에 대한 상세분석 및 보고자료 제공
  - ❖특정시간대의 네트웍 사용이력에 대한 분석자료 제공
  - ❖실시간 침입통계 자료에 의해 유해트레픽 자료 제공
- ❑시스템에 대한 사용 내역 및 통제 기능 구현가능
- ❑외부로부터 인터넷을 통한 바이러스, 해킹 접근을 분석 / 통제
- ❑네트웍 재해에 대한 사용자 역추적 기능 및 대응으로 관리자의 업무를 최소화

INFO

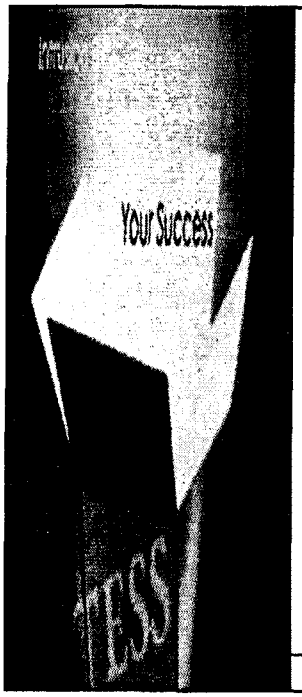
대학네트웍 침입탐지시스템을 왜 도입하는가??

TESS

TESS는 재해방지시스템



INFO



TESS

1. Overview
2. 제품주요기능
3. Reference

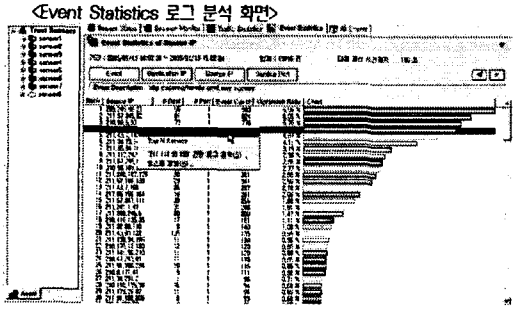
제품주요기능

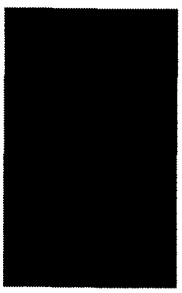
TESS

실시간 침입통계 자료에 의한 분석

- ✓ 실시간 네트워크 유해트래픽에 대한 통계자료 제공
- ✓ 최대공격패턴, 최대피해 시스템, 최대공격자 및 최대피해 포트에 대한 실시간 통계자료 제공
- ✓ 네트워크 재해에 대한 최초의 정보제공 - 사용자 역추적 기능 및 대응방안 제공

<Event Statistics 로그 분석 화면>



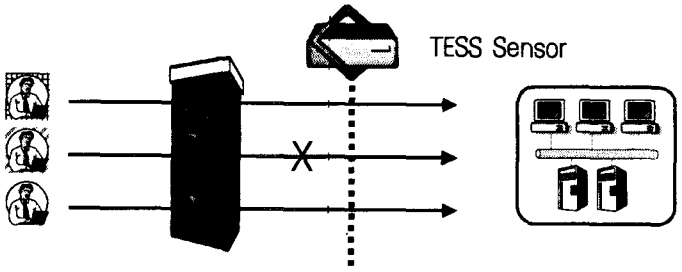


제품주요기능

TESS

분석된 자료에 의한 사용 제한 설정

- ✓ 공격대상, 공격자, 서비스에 대한 유해요소 탐지에 대한 대응책 제시
- ✓ 최대위험요소를 순차적으로 제거함으로써 네트워크의 안정성 추구
- ✓ 1.25 대란에서 보여준 특정 서비스에 대한 특정 포트 공격차단 – 침입탐지시스템으로만 탐지대응(네트워크 정책 설정 및 방화벽 연동 설정)



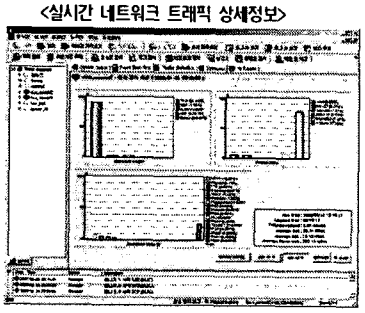
제품주요기능

TESS

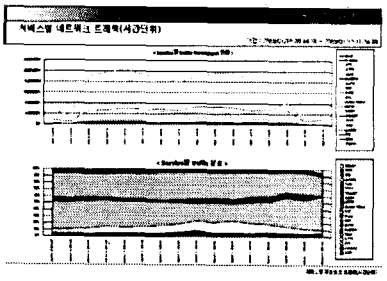
실시간 트래픽 정보 제공

- ✓ 실시간 프로토콜별, 패킷사이즈별, 서비스별 통계자료 제공
- ✓ 사용자 서비스 설정 가능(특정 서비스 특정 포트)
- ✓ 실시간 네트워크 트래픽 및 패킷 세션에 대한 정보 제공
- ✓ 특정 시간대별 네트워크 사용량에 대한 실시간 정보 제공

<실시간 네트워크 트래픽 상세정보>



<시간별 네트워크 사용량 조회>

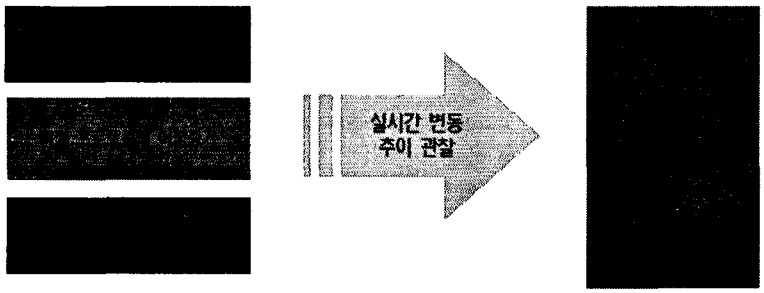


제품주요기능

TESS

네트워크 변화추이에 의한 이상징후 알림

- ✓ 최근 유행하는 공격의 경우 웜 등에 의한 서비스거부(DoS)공격이 주류
- ✓ 네트워크 트래픽이 갑자기 증가하는 경우 이상 징후로 판단
- ✓ 침입탐지시스템 – 네트워크 침입탐지 정보와 함께 이상징후 정보제공



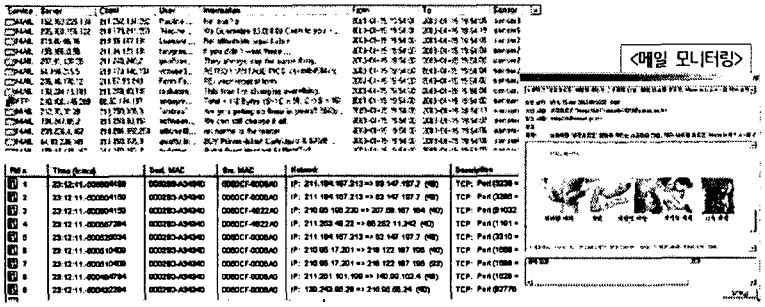
제품주요기능

TESS

세션 모니터링에 의한 서비스 감시

- ✓ 실시간 서비스 내용 조회 – SMTP, POP3, TELNET, FTP
- ✓ 메일, 메신저의 등의 내용을 실시간 감시 가능
- ✓ 사용한 트래픽에 대한 상세정보 실시간 조회

<트래픽 로깅 조회>



<메일 모니터링>

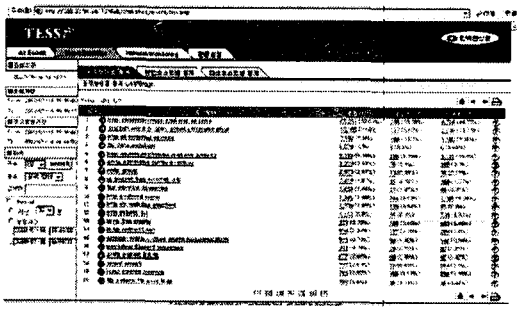
제품주요기능

TESS

웹 클라이언트에 의한 원격 감시

- ✓ 센서의 제어권을 제외한 모든 기능의 웹 관리 가능
- ✓ 트래픽 변동 추이 및 유해트래픽에 대한 상세 정보 제공에 의하여 외부에서도 이상징후에 대해서 감시가 가능

<웹 클라이언트>



제품주요기능

TESS

기타 기능

탐지기능

- 사용자 정의 해킹패턴 정의 기능 – 해킹패턴 1500개 이상
- 온라인 자동 업데이트 새로운 공격 가능성에 대한 경고 메일 발송
- 탐지된 공격에 대한 상세정보 제공 및 대응책 제시

관리기능

- 자동 백업 기능 및 사후 재현 기능
- 해킹 패턴별 대응기능 상세 설정(알람 및 방화벽 연동)
- 특정패턴 및 공격에 대한 정책설정 가능(방화벽 대용 기능)

대응기능

- 방화벽의 모든 서비스와 연동하는 지능형 시스템 → 침입방지시스템 기능수행
- IP-Wall 에 의한 자체 침입차단 시스템 내장
- ESM, NMS와 연동하는 통합관리 방안 제공(이글루 Spider-1, IBM RM.....)

TESS

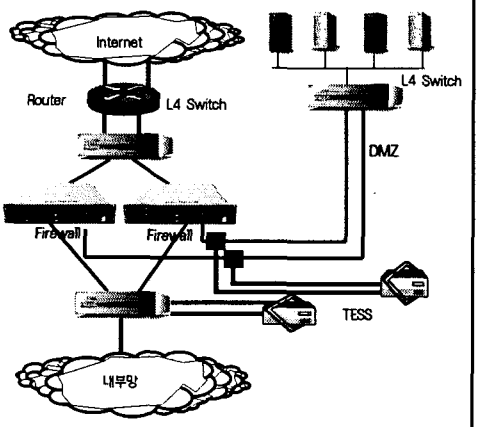
1. Overview
2. 제품주요기능
3. Reference

Reference

TESS

사례를 통한 구축방안(Gigabit Network) – I 대학교

1) DMZ쪽 Switch 와 방화벽 사이에 Tap장비를 연결하여 IDS설치
2) 방화벽내부 L4 Swith에 1:1로 각각 미러링하여 Packet Capture
3) 내부망에 통합 관리 Manager를 설치하여 통합 관리.
4) DMZ 내부의 중요 서버(전자결제, BBS서버 등)들에 대하여 별도의 Viwer를 만들어 침입탐지 로그 관리
5) 방화벽과 연동하여 중요 침입에 대하여 차단



INFO

- 15 -

Reference

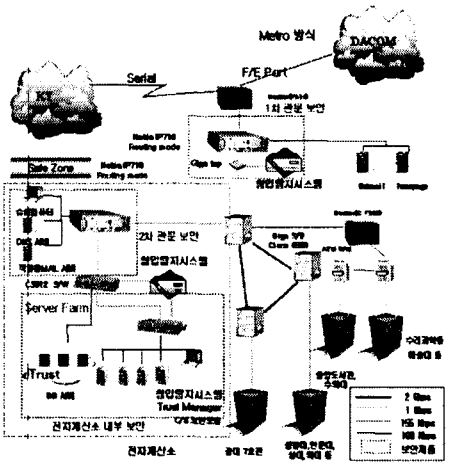
TESS

사례를 통한 구축방안(Gigabit Network) – J 대학교

1)1안의 특징은 슈퍼 컴퓨터 , 웹메일 서버 , 홈페이지를 제외하면 , 대부분 사용자들이 방화벽 도입 후에 별도의 설정이 불필요한 구축 방식이다.

2)슈퍼 컴퓨터는 외부의 대학등에서도 접속 사용하므로 , 학교 요구사항을 반영하여 별도의 DMZ 에 구축하였다. 이 과정에서 100 MEGA NIC 카드2개가 필요한데 이부분은 방화벽 NOKIA 에 장착된 4개의 100M NIC 카드를 이용.

3)1안의 특징 중에 하나는 2TH IDS 에서 C 3512 및 L2 및 GIGA 미러링 수행 필요하다. 각 스위치는 기가 미러링 가능하고 ,기가 포터 있는 상황



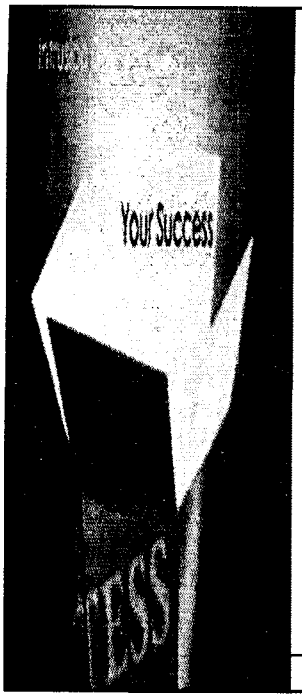
Reference

TESS

주요납품실적

• 국내 약 80여개 구축 사이트 보유 / TESS Giga 구축사이트는 굵은글씨 표시

구분	납품현황
공공기관	한국전산원(Giga), 경찰청 사이버테러대응센터, 근로복지공단, 서울시 전산본부, 건설교통부, 보험개발원, 국회도서관, 환경관리공단, 정보보호진흥원, 월드컵조직위원회, 한전KDN, 전기공사협회, 한국전자부품연구원, 한국전자통신연구원, 한국도로공사, 산림조합중앙회, 국제교류진흥회 등
금융기관	신영증권, 서울증권, 동부증권, KGI증권, 동양생명, 흥국생명, 고려상호저축, 세누리상호저축, 생명보험협회 등
일반기업 및 통신	데이콤(초고속국가망, Gateway(Giga), 사업용, 내부망), 두루넷(국제망 Giga), 이소프팅, 롯데건설, 쌍오텍, KIDC, KCC금강고려, 대우조선, B2B Internet, CIC Korea, 한국무역정보통신(Giga), 금강고려건설, 항용자동차, DIP Lab, 신호제지, 동양기전, 리브로닷컴, 대우종합기계(Giga), 위즈게이트, 용평리조트, 한국제지, 태광산업 등
대학교	전북대학교(Giga), 인천대학교(Giga), 인하대학교, 명지대학교, 항공기능대, 경북대병원, 영남이공대, 동원대학, 경일대학, 기능대학교 등
보안컨설팅 및 보안 SI사업	인천국제공항공사, 근로복지공단(보안컨설팅), 경찰청(사이버테러대응센터), 데이콤(국가망), 서울시청(전산정보관리소), 건설교통부(강제보험), 보험개발원, 정보통신부, 녹십자(VPN, IDS), KGI증권, 한국증권전산(정보공유센터) 등



TESS

감사합니다

INFOSEC