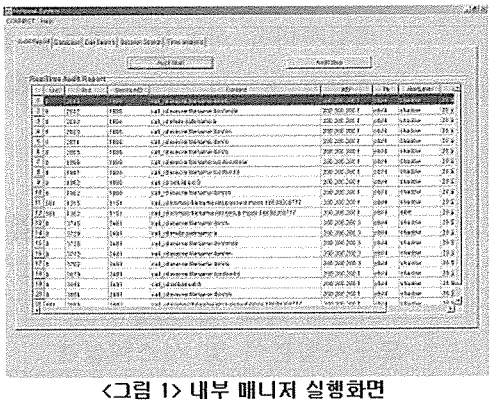
Fishbowl

"Fishbowl : 침입 탐지 및 감시 시스템"



<그림 1> 내부 매니저 실행화면

(주)비트컴퓨터(www.bit.co.kr)와 상명대학교가 공동으로 개발한 Fishbowl(침입 탐지 및 감시 시스템)은 실시간으로 장시간 침입자를 감시함으로써 행동패턴을 파악할 수 있도록 고안된 새로운 개념의 소프트웨어이다.
기존의 시스템이 침입자를 발견하면 접속을 차단하는 단순대응 위주로 제작이 된데 반해 Fishbowl 시스템에서는 단순한 대응의 개념을 뛰어넘어 좀 더 지능적인 대응이 가능토록 설계되었다. 즉, 지금까지의 소극적인 방법에서 벗어나 비정상적인 사용자를 가상의 공간(shadow file system)에 강제로 위치시켜 시스템의 보호 및 침입자의 행동패턴 분석하여 침입자의 기술수준과 공격의도를 파악, 관리자가 침입자를 관리할 수 있는 적극적인 개념의 방법을 채택하였다.
Fishbowl 시스템은 해킹을 당하고 있는 순간에도 서비스를 지속하는 철저한 시스템 보호를 기반으로 침입 정보의 수집을 하여 침입에 사용된 취약점을 식별하고 해당 취약점을 보완할 수 있으며 해커의 행적을 수집하고 추후 이것을 증거물로 제시할 수 있도록 구현되었다.
Fishbowl 시스템의 가장 큰 장점은 침입자에 의한 공격에 안전하다는 점이다. 침입자의 공격은 가상의 공간에만 적용이 되고 실제 파일 시스템에 영향을 미치지 못할 뿐 아니라, 침입자는 이를 인식하기 어렵다. 따라서 침입자는 마음껏 활동하고 난 후, 목적을 달성했다고 생각하지만, 실제로는 그의 행동이 Fishbowl 시스템의 감시 하에서 이루어지는 것이다.
또한 침입자가 공격을 하는 중이라도 이는 Shadow 파일 시스템에만 적용될 뿐 실제 시스템에 적용이 되지 않으므로, 계속적인 서비스 제공이 가능하다는 장점이 있다.
Fishbowl이라는 개념은 아직까지 실험적인 시도에 머무르고 있는 상태이나, 본 프로그램에 이를 적용, 구현하여 새로운 보안 솔루션의 방향을 제시하고 있다.

문의: 3486-3456 담당: 봉재훈

장 려 상

Fishbowl : 침입 탐지 및 감시시스템

1. 작품명 : Fishbowl : 침입 탐지 및 감시 시스템

2. 제작자 : (주) 비트컴퓨터 • 상명대학교

대 표 자 : 조현정

개발참여자 : 이정민, 봉재훈, 홍진석, 여욱형, 전건웅, 권준일, 김한겸, 김상욱, 백선욱, 추장우 외 8명

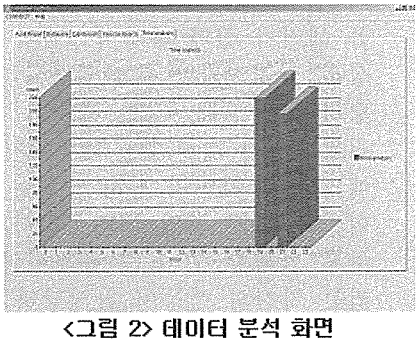
주 소 : (137-858) 서울 서초구 서초동 1327-33

전 화 : 02) 3486-3456

팩 스 : 02) 3486-7890

E - m a i l : chizeta@bit.co.kr

3. S/W 요약설명



<그림 2> 데이터 분석 화면

본 시스템에서 침입자라고 판단된 사용자는 실제 시스템과 모든 환경이 일치하는 가상의 시스템(Shadow File System)으로 옮겨지고 모든 행위를 감시한다. 즉, 침입자의 행위는 모든 행동이 로그 파일로 기록에 남겨지게 된다. 이것을 바탕으로 모든 상황을 실시간 모니터링하여 관리자가 침입자의 행동패턴을 분석할 수 있으며, 침입자의 기술 수준과 침입 의도를 판단하여 침입자를 관리 할 수 있도록 하였다. 침입자에

의한 모든 행위는 실제 시스템이 아닌 가상의 시스템에서 이루어지므로 실제 시스템은 아무런 영향을 받지 않게 된다. 또한 가상의 시스템과 관련된 모든 기능과 파일을 은닉하여 가상의 시스템의 존재를 감추어서 어떤 사용자라도 가상 시스템의 존재를 인식하지 못하도록 설계되었다.

4. 개발 배경

현재 해커들의 공격을 막기 위한 보안 솔루션으로 널리 사용되고 있는 것은 방화벽과 이 방화벽의 단점을 개선한 침입탐지 시스템(IDS: Intrusion Detection System)이다. 그러나, 방화벽은 서비스 포트 검색에 의한 간단한 접근 제어만 할 수 있으며, IDS의 차후 공격에 대비한 자료수집 및 단순한 접속차단 정도의 기능만 가지고는 점점 지능화되어 가는 최근의 해킹기술을 차단하는데 한계성을 드러내고 있다.

이러한 기존 보안 시스템의 한계를 극복하기 위해서는 부정행위자를 색출하여 고발하는 등의 보조 수단 확보가 필요하다. 예를 들어 해커들이 인식하지 못하는 상태에서 그 활동을 장시간 감시하고 해커들의 침입패턴을 분석함으로써 해커의 신원파악까지 할 수 있는 기능들을 필요로 하고 있다.

본 프로그램은 시스템의 정보를 안전하게 보호하면서도 해커의 행동방식에 대한 정보 수집 능력 강화에 초점을 맞춘 새로운 개념의 침입 대응 시스템이다. 본 프로그램에서 개발된 Fishbowl 기능은 해커가 실제 파일시스템이 아닌 Shadow File System이라는 가상의 작업공간에서 작업하도록 함으로써 실제 파일시스템은 공격당하지 않도록 하고, 해커의 행동방식을 감시하여 침입자에 대한 정보수집이 실시간에 이루어지도록 하고 있다. Fishbowl 시스템 내에 구현된 IDS의 감사 모듈은 이러한 자료를 수집하며, 대응 모듈이 적절하게 침입에 대응한다. 더 나아가 침입의 패턴을 분석하여 차후 발행할 수 있는 유해행위를 미연에 방지할 수 있다. 또한, 해커는 자신의 행동이 감시당하고 있다는 사실을 파악하지 못하도록 시스템의 주요정보들을 은닉하고 있으며, 해커의 공격행위 상태에서도 정상적인 사용자들에게는 지속적인 서비스를 제공할 있는 장점이 있다.

5. 시스템 개요

IDS의 탐지 모듈에 의해 침입자로 판단된 사용자는 침입대응 및 분석 시스템 내부의 가상공간(Shadow File System)에 위치하게 되며, 모든 행위를 철저히 감시당한다. 시스템 내로 들어온 비정상 사용자는 시스템의 취약점을 이용해 루트권한을 얻은 후, 데이터를 삭제하거나 복사한다. 때때로 시스템을 파괴하기 위해서 모든 데이터를 지우기도 하고, 침입 흔적을 없애기 위해 로그파일을 수정하거나 백도어를 설치해 둘 수도 있다. 그러나 이러한 행위는 커널의 철저한 감시를 받게 되므로 비정상 사용자의 모든 행동이 로그파일로 기록에 남게 되며, 이러한 데이터를 바탕으로 행동패턴을 파악하게 된다.
비정상 사용자에 의한 모든 행위는 실제 시스템이 아닌 가상의 시스템에서 이루어지므로 실제 시스템은 아무런 영향을 받지 않게 된다.

6. 시스템 특징

1. 위험 등급별로 침입자 IP 차단 및 관찰을 통한 행동패턴 파악 등 다양한 침입대응 방식을 제공한다.
2. 침입자의 공격을 Shadow File System을 이용하여 무력화시킴으로써 실제 파일 시스템에 영향을 미치지 못하도록 하여, 시스템의 안전성을 확보한다.
3. 침입자의 공격 중에도 신뢰성 있는 서비스가 가능하다.
4. 접속을 유지한 채 감시하므로, 침입자를 장시간 관찰이 가능하도록 하여 행동패턴 파악에 매우 유리하다.
5. 실시간으로 상세한 감사자료를 생성하고, DB에 저장하여 행동패턴 분석의 자료로 활용한다.
6. 이식의 가능성을 고려하여 모듈로써 구현하였다.
6. 실제 파일 시스템과의 환경일치로 시스템 노출의 가능성을 최소화한다.

타제품과의 성능비교

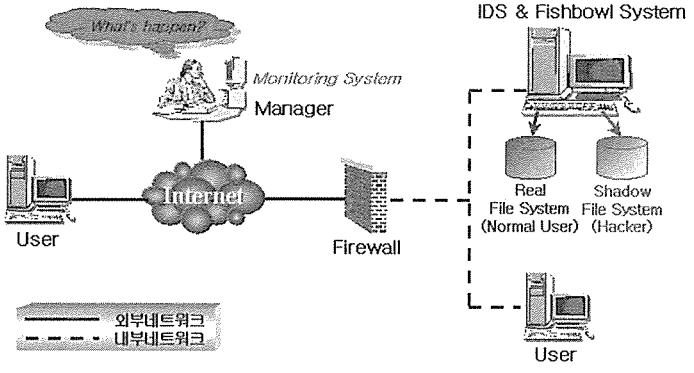
1. 적극적인 침입대응 방식
2. 침입자 발견시 접속을 유지한 상태로 장시간 감시

3. 시스템 안전성 확보
4. 지속적인 서비스의 보장

우수성 및 시장성

1. 현재 실험적인 시도에 머무르고 있는 Fishbowl의 개념을 적용하여 구현함으로써 새로운 방향제시
2. 최근에는 침입에 대한 좀 더 적극적인 대응방식을 요구하는 추세이므로 본 프로그램에서 사용된 기술 적용시 기술선점의 효과
3. 별도의 장비없이 하나의 시스템 내에 구현함으로서 비용절감 및 효율적 관리

7. 시스템 구성



<그림 3> 전체 시스템 구성도

그림을 보면, 내부 사용자는 로컬 네트워크 환경을 통하여 Fishbowl 시스템에 로그인을 하게 되며, 외부 사용자는 인터넷을 통해 일차적으로 방화벽을 거쳐 Fishbowl 시스템에 로그인하게 된다. 로그인한 사용자들 중에서 IDS에서 침입자로 탐지된 사용자는 Shadow 파일 시스템으로 옮겨지게 되고, 실제 파일 시스템은 보호받게 된다. 또한, 그림의 매니저는 Fishbowl 시스템과 전체 네트워크 망을 감시한다. 좀 더 구체적인 각 부분별 동작은 다음과 같다.

1. Fishbowl & IDS 시스템

   IDS와 Shadow File System이 구현된 곳으로서, 침입자의 탐지,

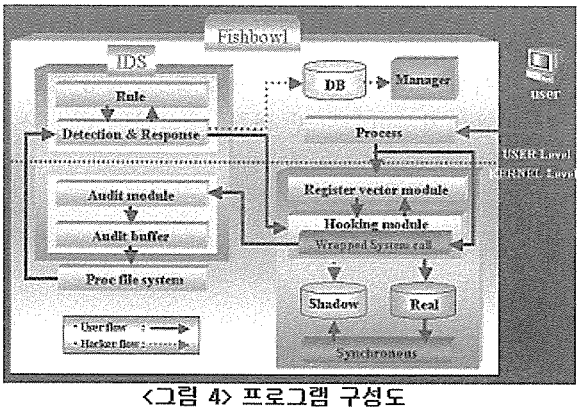
Shadow File System으로의 유도 및 침입자를 감시한다. 정상사용자는 실제 파일 시스템에서 정상적인 동작을 수행하고, 침입자는 Shadow File System에서 감시를 받으며 동작을 하게 된다. 정상사용자와 침입자의 작업공간을 분리시킴으로써 시스템을 보호하게 된다.

2. 방화벽 (Firewall)
   전체적인 내부 네트워크 망에 대한 패킷 필터링을 수행한다. 사용하지 않는 모든 네트워크 서비스 포트는 기본적으로 막게 되며 허용 포트만 열게 된다.
3. 매니저
   실시간으로 변화하는 Fishbowl 시스템의 상황을 관리자 화면을 통해 출력하며, 내부 네트워크 망(내부 매니저) 또는 외부 네트워크 망(외부 매니저)에 위치할 수도 있다.

8. 주요 기능

본 프로그램의 모든 기능들은 모듈 프로그래밍으로 작성하여 이식성을 높였으며, 모듈간의 최적의 통신을 최대한 고려하였다. 각각의 기능들에 대해서 좀 더 자세하게 살펴보면 다음과 같다.

1. Shadow File System
   정상사용자와는 달리 침입자에 의해 이루어지는 모든 작업은 실제 파일 시스템이 아닌 Shadow File System에서 이루어지게 된다. 따라서 침입자에 의한 모든 행위는 실제 시스템에 아무런 영향도 미치지 못한다.



<그림 4> 프로그램 구성도

2. 침입 탐지 시스템 (IDS : Intrusion Detection System)
   오용 탐지 기법을 이용하여 룰 파일과 침입 패턴을 비교하여 침입자

를 탐지한다. 룰 파일의 생성은 동적 라이브러리 기법을 이용한다.

3. 방화벽 (Firewall)
   전체적인 내부 네트워크 망에 대한 패킷 필터링을 수행한다. 사용하지 않는 모든 네트워크 서비스 포트는 기본적으로 막게 되며 허용 포트만 열게 된다.
4. 시스템 정보은닉
   시스템의 중요한 정보에 대해서는 철저한 은닉이 요구된다. 이에 본 프로젝트에서는 연결리스트를 제어함으로써 중요한 모든 모듈들과 파일들에 대해서는 은닉한다.
5. 사용자의 프로세스 목록 저장
   모든 사용자의 프로세스 목록을 특정 자료구조에 저장한다.
6. 사용자와 침입자의 구분
   정상사용자와 IDS에서 탐지된 침입자를 구분한다. 정상사용자는 실제 시스템 콜을 사용하도록 하고, 침입자는 Fake 시스템 콜을 사용하도록 분리시켜 준다. 좀 더 구체적으로 말하면, 침입자의 프로세스는 정상사용자의 프로세스와는 달리 본 프로젝트에서 구현한 Fake 시스템 콜을 사용하게 되어 실제 파일 시스템이 아닌 Shadow 파일 시스템에만 접근하도록 한다.
7. 커널 레벨의 감사 자료
   모든 사용자의 행위를 실시간으로 커널레벨의 감사 자료를 생성할 수 있도록 구현하였다. 또한, 이 모든 감사 자료는 DB화된다.
8. 내부 및 외부 매니저
   Fishbowl 시스템의 리눅스 환경에서 작동하는 내부 매니저와 외부 네트워크의 윈도우 환경에서 작동하는 외부 매니저를 구현하였다. 관리자는 내부 및 외부 매니저에서 시스템을 감시하고 관리할 수 있다.

9. 개발단계별 기간 및 투입인원수

개발단계	개발시간	인원	비고
시스템 계획	2001.10 ~ 2001.12	7	시스템의 안전을 고려한 보안 솔루션 제작
시스템 설계	2002.1 ~ 2002.2	4	하나의 시스템 내에 구현
프로그래밍	2002.3 ~ 2002.7	7	시스템의 부하를 최대한 감소
테스트 및 수정	2002.8 ~ 2002.9	7	다양한 방법을 적용하여 테스트
매뉴얼제작	2002.9	2	사용자 매뉴얼 제작
계	12개월	18	

10. 사용 시스템과 개발언어

구 분	사 양	비 고
OS	Redhat Linux 7.3	Kernel version 2.4.18
Process	PIII 1Ghz	Intel
RAM	512MB	
개발언어	gcc 2.96, Java	