정보보호

(5111041)

8장

침입탐지

침입자

- 가장 대표적인 보안 위협의 두 가지는 악성코드와 침입자
- 일반적으로 해커 또는 크래커를 일컬음

- 분류:

위장된 사용자 (masquerader)	직권 남용자 (misfeasor)	비밀 사용자 (clandestine user)
• 외부 소행자 • 합법적인 사용자 계정을 이용하기 위해 시스템에 침투하는 허가되지 않은 사용자	• 내부 소행자 • 권한을 악용하는 합법적 사용자	• 외부 소행자, 내부 소행자 • 감사와 접근제어를 회피하거나 감사 수집(audit collection)을 억제하기 위해 감독 제어를 몰수 하는 사용자

침입의 예

- 원격 루트 손상
- 웹서버 훼손
- 패스워드 추측/크랙킹
- 신용카드 번호를 포함하고 있는 데이터베이스 복사
- 허가 없이 민감한 데이터 엿 보는 행위
- 패킷 스니퍼(sniffer) 실행
- 불법복제 소프트웨어 배포
- 보안되지 않은 모뎀을 사용하여 내부 네트워크 접근하는 행위
- 정보 취득을 위한 위장
- 허가 없이 워크스테이션 사용을 사용하는 행위

해커

- 시스템에의 접근이나 그에 따른 지위에 대한 희열에 동기가 부여되어 그러한 기술 개발에 정열을 쏟는 고급 기술자
  - 해킹 커뮤니티는 뛰어난 실력자 층
  - 지위는 능력 수준에 따라 결정됨
- 침입자는 자원을 소비하여 합법적인 사용자의 시스템 성능을 저하시킴
- 침입 탐지 시스템(IDSs)와 침입 방지 시스템(IPSs)는 해커의 위협을 감지 하기 위해 고안됨
  - 특정 IP주소로의 원격 로그온을 제한 할 수 있음
  - 가상 사설망(VPN)을 사용할 수 있음
- 침입자 문제는 컴퓨터 긴급 대응 팀(CERTs)의 설립을 선도함

해커 행동 패턴

1. • NSLookup, Dig, 기타 등등 IP 룩업 도구를 사용하는 타겟 선정
2. • NMAP와 같은 툴을 이용하는 접근 가능한 서비스에 네트워크를 맵핑 시킴
3. • 잠재적으로 취약한 서비스 식별 (이 경우, PC애니웨어 이용)
4. • pcAnywhere의 패스워드를 추측(brute force)
5. • DameWare와 같은 원격 관리 도구 설치
6. • 관리자가 로그온 하여 패스워드를 캡쳐해냄
7. • 알아낸 관리자 패스워드로 나머지 네트워크 시스템에 접근

범죄조직

- 현재 위협을 주는 해커들로 조직된 그룹
  - 기업 / 정부 / 느슨하게 연계된 조직
  - 일반적으로 어림
  - 대게 동유럽, 러시아 또는 동남 아시아 해커들이 많음
  - 주로 언더그라운드 포럼에서 만남
  - 보통 전자상거래 서버상의 신용카드 파일을 타겟으로 함
- 범죄 해커는 대체로 특정 타겟을 가지고 있음
  - 사이트에 침투하면 공격자는 빠르게 행동을 취해 정보를 빼냄
- IDS / IPS 가 사용될 수 있지만 효과적이지 못함
- 민감한 데이터는 암호화되어야 함

범죄 조직의 행동 패턴

빠르게 행동을 취하며 그들의 활동을 탐지되기 어렵게 함

취약한 포트 주변을 이용함

재 진입용 백도어를 남기기 위해 트로이의 목마(숨겨진 소프트웨어)를 설치

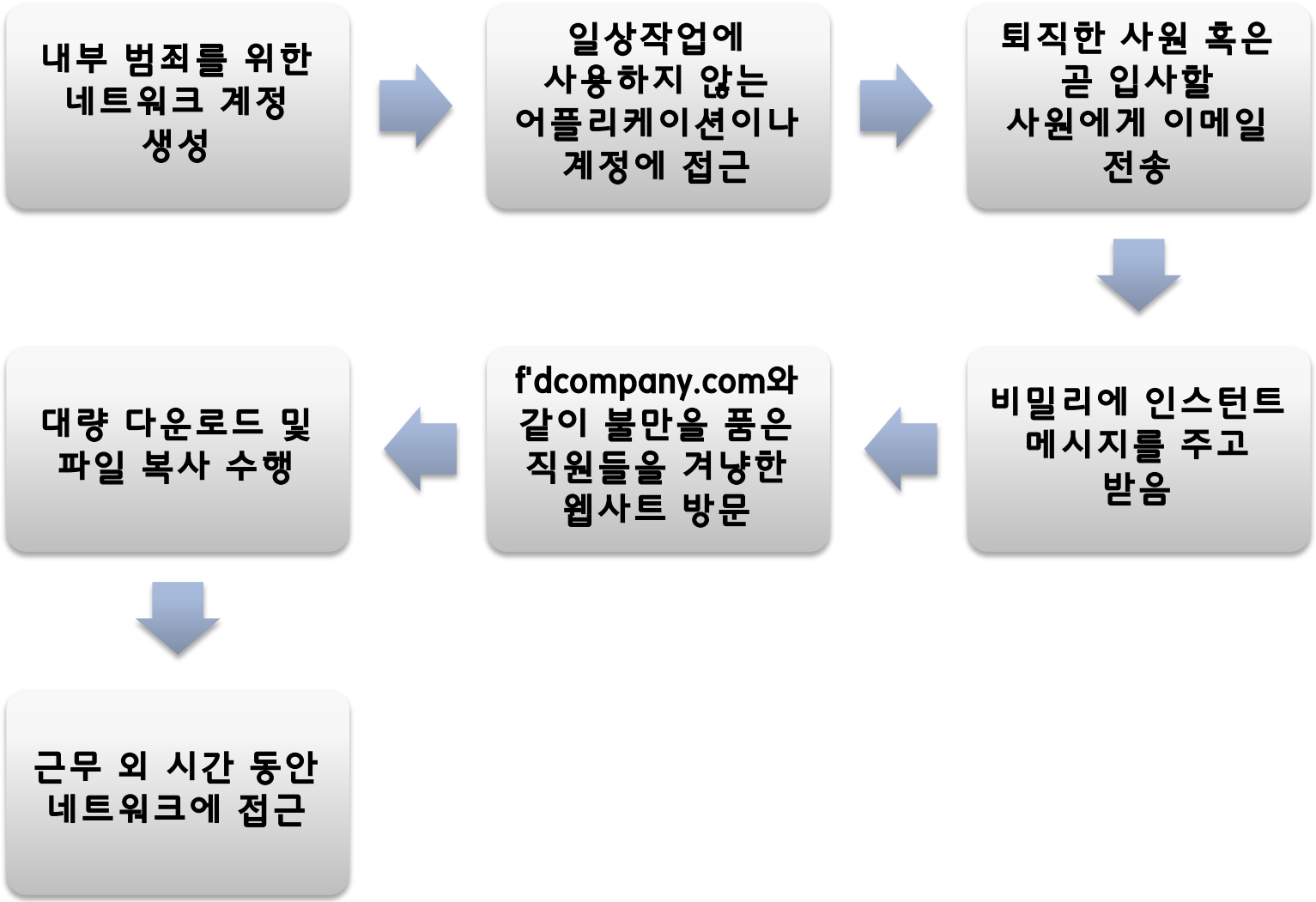
패스워드 캡쳐를 위해 스니퍼를 사용함

발견될 때 까지 머물지 않음

내부 범죄

- 탐지와 예방이 가장 어려움
- 접근 권한과 시스템에 대한 지식을 소유하고 있음
- 보복을 목적으로 하거나 권한에 의해 동기가 부여 될 수 있음
  - 고용기간이 만료되어 경쟁사로 이직할 때, 고객 정보를 빼내감
- IDS / IPS는 유용할 뿐만 아니라 필요 됨:
  - 최소 권한강화, 로그 모니터링, 강력 인증, 터미네이션 처리

내부범죄의 행동패턴


내부 범죄를 위한 네트워크 계정 생성
일상작업에 사용하지 않는 어플리케이션이나 계정에 접근
퇴직한 사원 혹은 곧 입사할 사원에게 이메일 전송
비밀리에 인스턴트 메시지를 주고 받음
f'dcompany.com와 같이 불만을 품은 직원들을 겨냥한 웹사트 방문
대량 다운로드 및 파일 복사 수행
근무 외 시간 동안 네트워크에 접근

RFC2828 (인터넷 보안 용어 사전)
침입 관련 논점:

보안 침입: 하나의 보안 사건, 또는 침입자가 행하는 보안 침해 사고나 허가 권한 없이 시스템(또는 자원)을 빼내거나 액세스 하려는 시도로 구성된 **다양한 보안 사건의 조합**

침입 탐지: 허가되지 않은 방식으로 시스템 자원에의 접근시도를 발견 및 실시간(또는 실시간 근접하게)으로 알려주는 목적의 시스템을 모니터링 하거나 분석하는 보안 서비스

침입탐지 시스템(IDSs)

- 호스트 기반 IDS
  - 호스트의 의심스러운 행위 특징들을 모니터링
- 네트워크 기반 IDS
  - 네트워크 트래픽을 모니터링하고 의심스러운 행위를 식별하기 위해 네트워크, 트랜스 포트, 및 어플리케이션 프로트콜을 분석

3가지 논리 구성요소:

- **센서 – 데이터 수집**
- **분석가 – 침입 유무에 대한 판정**
- **유저 인터페이스 - 산출물이나 제어 시스템의 행위를 보여줌**

IDS 원칙

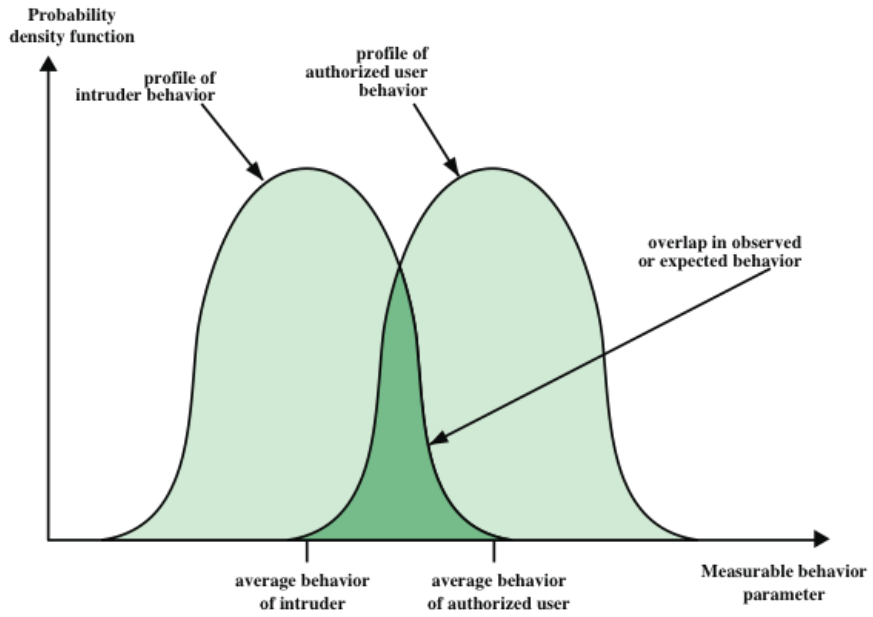


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

- 침입자의 행위는 합법적 사용자의 행위와 다른 양상을 띰
- 행동의 중복이 문제를 야기시킴
  - 가긍정적 판단
  - 가부정적 판단

IDS 요구사항

지속적인 동작	결함 포용능력 (fault tolerant)	침입 시스템 자체의 견고함 (resist subversion)
시스템에 가해지는 부하의 최소화	보안정책에 따른 환경 설정	시스템과 사용자의 변화에 대한 적응
많은 수의 시스템 모니터링을 위한 크기 변경	최소한의 서비스 저하	동적 재설정 허가

호스트 기반 IDS

- 취약하거나 민감한 소프트웨어에 대해 보안소프트웨어 전문 계층을 더해줌
- 의심스러운 행위를 탐지하기 위해 활동 모니터링
  - 주요 목적은 침입 탐지, 의심스러운 이벤트 기록 및 경고 전송
  - 외부침입 내부 침입 모두를 탐지할 수 있음

침입 탐지에 대한 호스트 기반 IDS 접근

이상 탐지

- 스레스홀드 탐지
  - 일정 시간 동안 특정 종류의 이벤트 발생 숫자를 계산
- 프로파일 기반
  - 각 사용자의 활동에 대한 프로파일이 만들어져 개인 계정의 행위 변화를 탐지하는 데 사용

시그니처 탐지

- 보여지는 행위가 침입자인가를 판별하기 위해 사용되는 일련의 규칙이나 공격 패턴을 정의

감사 기록
(Audit Records)

네이티브 감사 기록

- 다중사용자 운영체제는 사용자 활동에 대한 정보를 수집하는 어카운팅 소프트웨어를 가지고 있음
- 추가적인 수집 소프트웨어가 필요 하지 않다는 것이 이점
- 필요한 정보가 포함되어 있지 않거나 복잡한 형식으로 기록될 수 있다는 것이 단점

탐지 – 특정 감사 기록

- IDS에 의해 요구된 정보만을 포함하고 있는 레코드를 발생시키는 수집 시설
- 기업이 독립적으로 만들 수 있고 다양한 시스템에 이식할 수 있다는 것이 이점
- 컴퓨터상에서 실제 실행 중이거나 문제가 있는 어카운팅 패키지와 연관된 추가 오버헤드가 단점

표 8.2

침입 탐지에 사용 되는 방법

측정기준	모델	침입의 종류
로그인과 세션활동		
로그인 빈도 (날짜, 시간별)	평균, 표준편차	침입자는 근무시간 외에 로그인 가능성이 높음
로그인 빈도 (위치별)	평균, 표준편차	침입자는 본래 사용자가 거의 혹은 전혀 접속하지 않는 위치에서 접속한다
마지막 로그인 시간	Operational	휴면계정을 이용한 로그인
세션의 시간	평균, 표준편차	평상시와 상이한 세션시간은 사용자를 가장한 침입이 수 있다
장소로의 데이터 전송량	평균, 표준편차	원격 위치로의 지나치게 많은 양의 데이터 전송은 중요한 정보의 누출를 의미할 수 있음
세션의 자원 이용	평균, 표준편차	평상시보다 많은 프로세서 및 I/O 사용량은 침입의 증거일수 있음
패스워드 실패	Operational	추측한 패스워드로 로그인 시도
특정 터미널에서의 접속 실패	Operational	침투 시도
명령어 또는 프로그램 실행 활동		
실행 횟수	평균, 표준편차	특별한 명령어를 사용하는 침입자 혹은 루트권한의 명령어를 사용할 수 있게 된 합법적인 사용자
프로그램 자원 사용	평균, 표준편차	비정상적인 자원사용량은 바이러스나 트로이목마가 침투해서 프로세서나 I/O사용량이 증가하는 효과를 일으킴
실행 거부	Operational	좀 더 높은 실행권한을 얻으려고 시도하는 사용자
파일 접근 활동		
읽기, 쓰기, 만들기, 삭제하기 빈도	평균, 표준편차	읽고 쓰기의 비정상적인 활동은 침입을 의미
레코드의 읽기/쓰기	평균, 표준편차	이상치는 추론이나 통합을 통하여 중요한 정보를 빼내려는 시도를 의미함
읽기, 쓰기, 만들기, 지우기의 실패	Operational	허가되지 않은 파일을 지속적으로 접근하려고 하는 사용자

시그니처 탐지 (Signature Detection)

- 규칙 기반 이상탐지
  - 사용 패턴을 식별하기 위해 수집된 감사 레코드가 분석됨
  - 그러한 패턴을 기술하는 규칙이 만들어짐
  - 현재 행위가 일련의 규칙에 매칭됨
  - 시스템 내부의 보안 취약점과 관련된 지식을 요구하지 않음
  - 규칙에 대한 대형 데이터베이스가 필요함

- 규칙 기반 침투 식별
  - 알려진 침투나 취약점을 이용한 침투를 식별하는 규칙의 사용한다는 점이 주요 특징
  - 규칙은 의심스러운 행위를 식별하는 것으로 정의됨
  - 일반적으로 규칙은 컴퓨터와 운영체제에 대한 구체화

Distributed Host-Based IDS

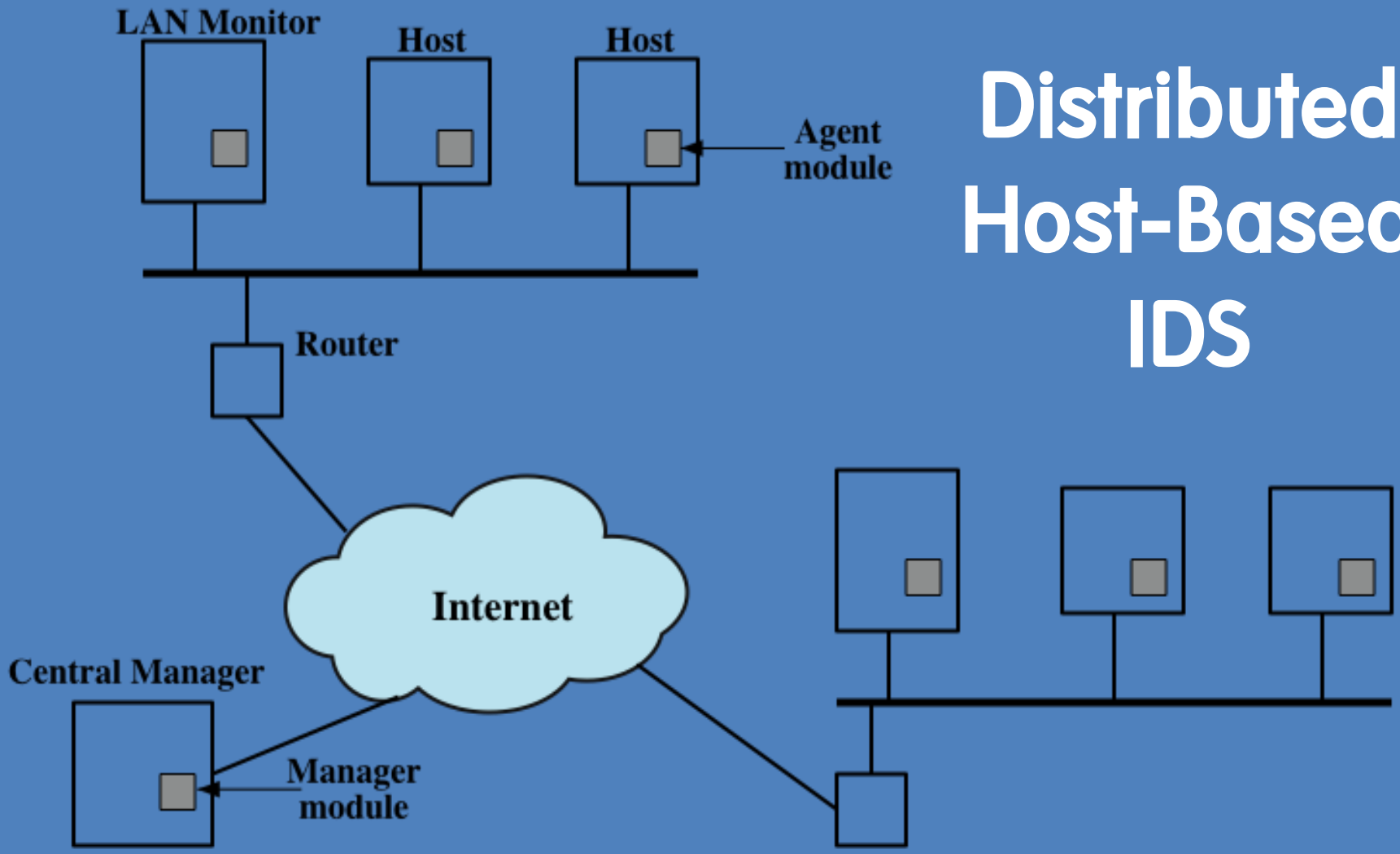


Figure 8.2 Architecture for Distributed Intrusion Detection

네트워크 기반 IDS (NIDS)

네트워크 상에서 선택된 지점의 트래픽 모니터링

실시간 또는 실시간에 근사한 속도로 트래픽 패킷 분석

네트워크, 트랜스포트, 또는 어플리케이션 레벨 프로토콜 행위 검사

많은 센서, 관리 기능에 대한 하나 또는 그 이상의 서버 및 휴먼 인터페이스에 대한 관리자 콘솔들로 구성됨

센서 및 관리 서버 또는 그 둘의 조합에서 트래픽 패턴에 대한 분석이 이뤄짐

NIDS 센서 배치

- 인라인(inline) 센서
  - 네트워크 세그먼트에 삽입되어 그 센서를 직접 통과하는 트래픽만 감지
- 수동(passive) 센서
  - 네트워크 트래픽 사본을 감시

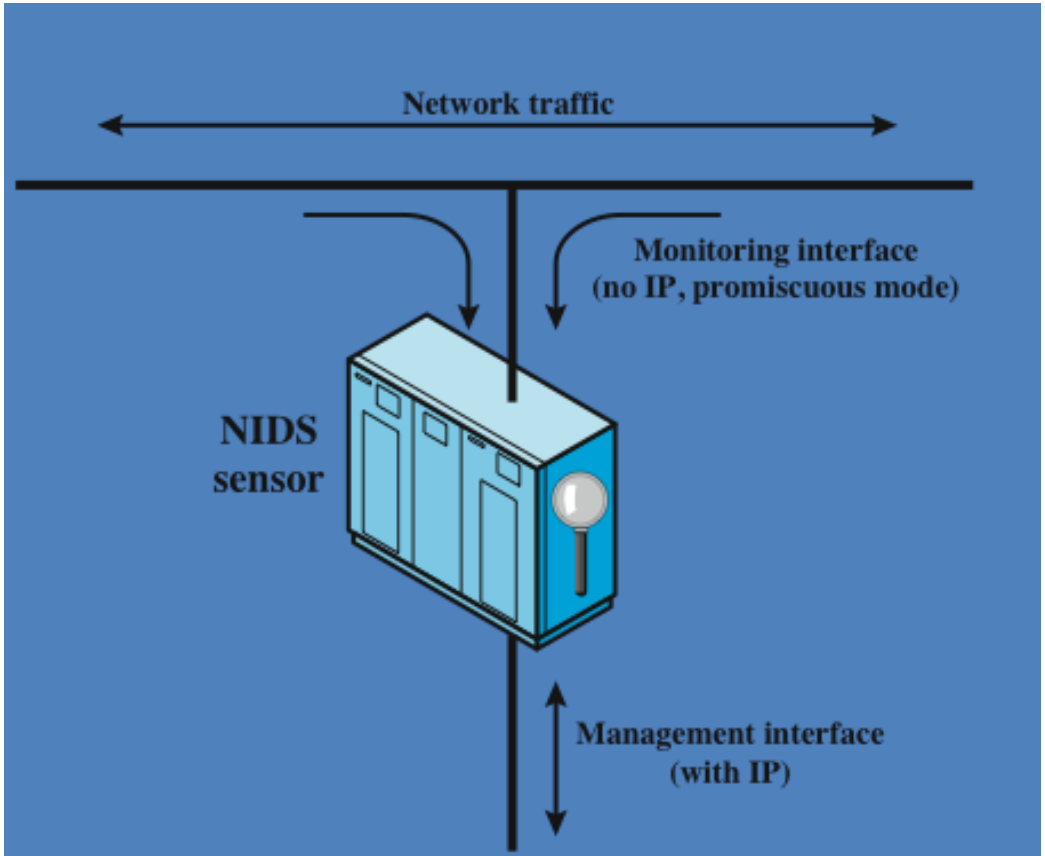


Figure 8.4 Passive NIDS Sensor (based on [CREM06])

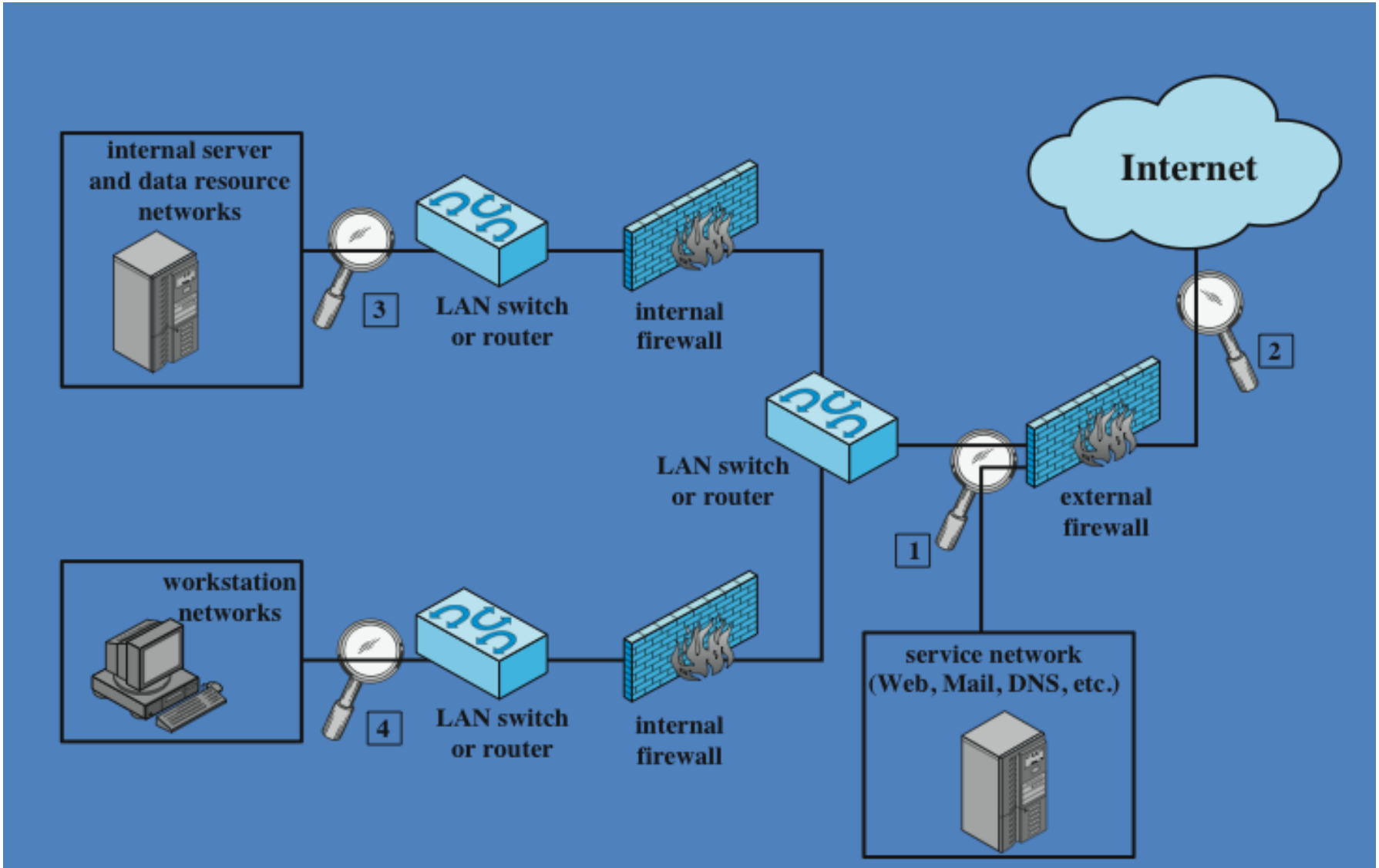


Figure 8.5 Example of NIDS Sensor Deployment

NIDS Deployment Scenarios

- Location 1 (외부 방화벽 안쪽)
  - 가장 흔한 위치
  - 외부 방화벽을 뚫고 오는 외부 공격 탐지
  - 내부의 감염된 서버로부터 외부로 나가는 트래픽 감지
- Location 2 (외부방화벽과 인터넷 사이)
  - 외부(인터넷)으로부터 대상 네트워크에 대한 공격 횟수, 종류 파악
  - 트래픽 처리 부담 ↑
- Location 3 (내부 네트워크 주변부)
  - 많은 네트워크 트래픽 감시 -> 공격 탐지 확률 ↑
  - 경계 내부의 허용되지 않은 행동 탐지
- Location 4 (워크스테이션 주변부, 중요 자산)
  - 중요 자산 집중

침입 탐지 기법

- 시그니처 탐지
  - 응용프로그램 계층, 트랜스포트 계층, 네트워크 계층; 예기치 못한 응용프로그램 서비스, 정책 위반
- 이상 탐지
  - 서비스 거부 공격, 스캐닝, 웜
- 센서가 잠재적 위협을 탐지하면 이는 경고를 전송하고 해당 이벤트와 연관된 정보를 로깅 함
  - 분석모듈은 침입탐지 파라미터와 알고리즘을 조정하기 위해 이러한 정보를 사용함
  - 보안 관리자는 예방기법을 설계하기 위해 이러한 정보를 이용할 수 있음

허니팟
(Honeypot)

- 의도된 유인 시스템:
  - 중요 시스템에서 멀어지도록 잠재 공격자 유인
  - 공격자의 활동에 관한 정복 수집
  - 관리자가 공격자에 대응할 수 있게 하기 위해 시스템 상에 오래 머물도록 꾐
- 합법적인 사용자가 접근하지 않는 정보들로 차 있음
- 생산 가치가 없는 자원
  - 시스템과 통신 시도의 대부분은 프로브, 스캐닝 또는 공격 임
  - 아웃바운드 통신이 시스템이 문제가 있을 거라고 제기함
- 일단 해커가 네트워크에 진입하게 되면 관리자는 이를 방어하기 위해 해커의 행위를 관찰 함

허니팟 배치

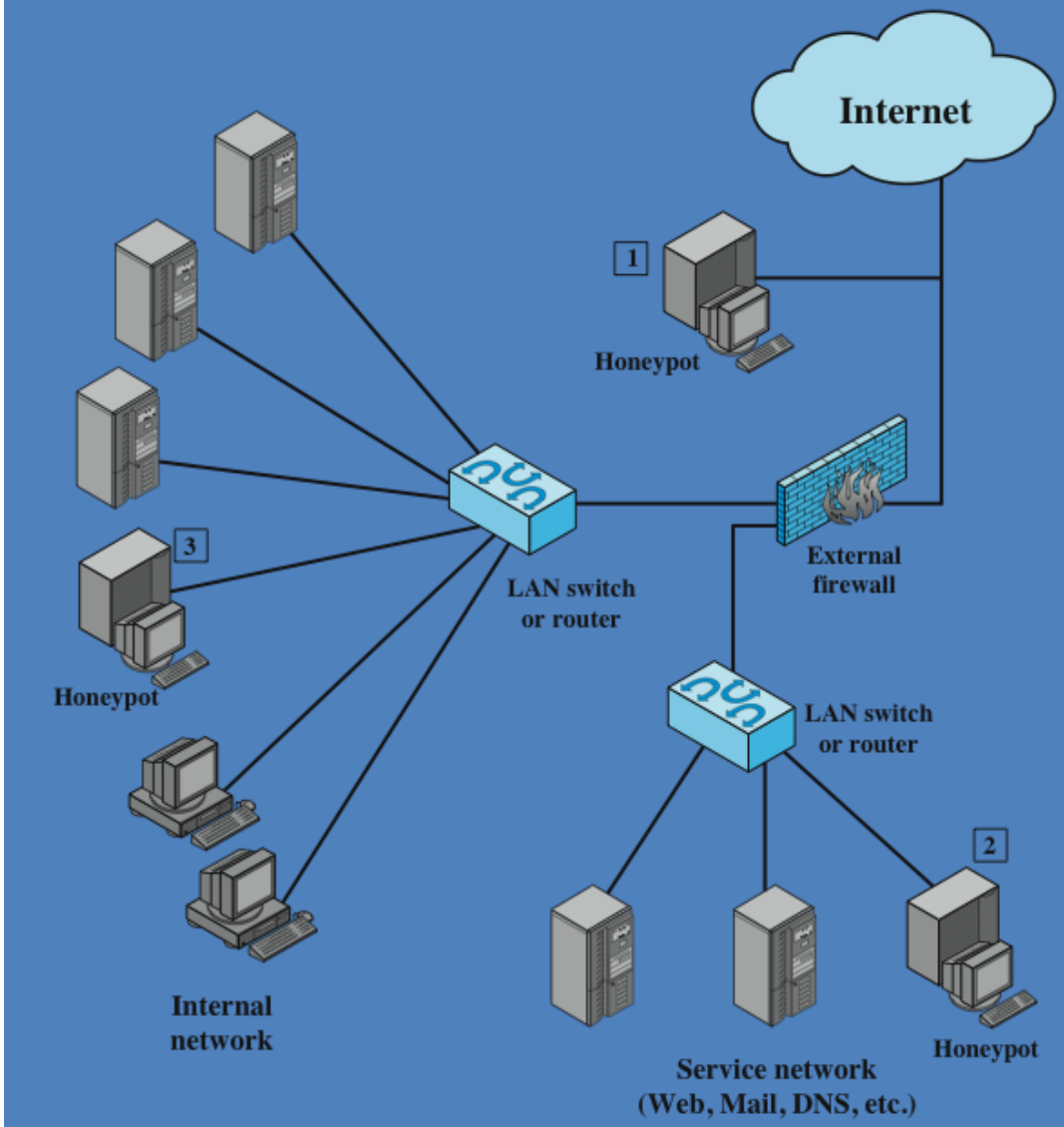


Figure 8.8 Example of Honeypot Deployment

Honeypot Deployment Scenarios

- Location 1 (외부 방화벽 밖)
  - 내부 네트워크 위험 증가 X
  - 내부 시스템 부하 최소화
  - 내부 공격자 확인 불가
- Location 2 (DMZ)
  - 외부접근이 가능한 내부 네트워크(웹서버, 메일서버 등)
  - DMZ 내 다른 시스템에 대한 보안성 향상 필요
  - 방화벽의 기능을 일부 해제해야 하므로 위험성 증가
- Location 3 (내부 네트워크)
  - 내부 공격 탐지 가능
  - 방화벽의 실수 탐지 가능
  - 잠재적 위험성 증가

스노트
(SNORT)

- 경량의 IDS
  - 실시간 패킷 캡쳐 및 규칙 분석
  - 노드 상에 쉽게 배치됨
  - 메모리 및 프로세서 시간의 사용량이 적음
  - 설정이 용이함

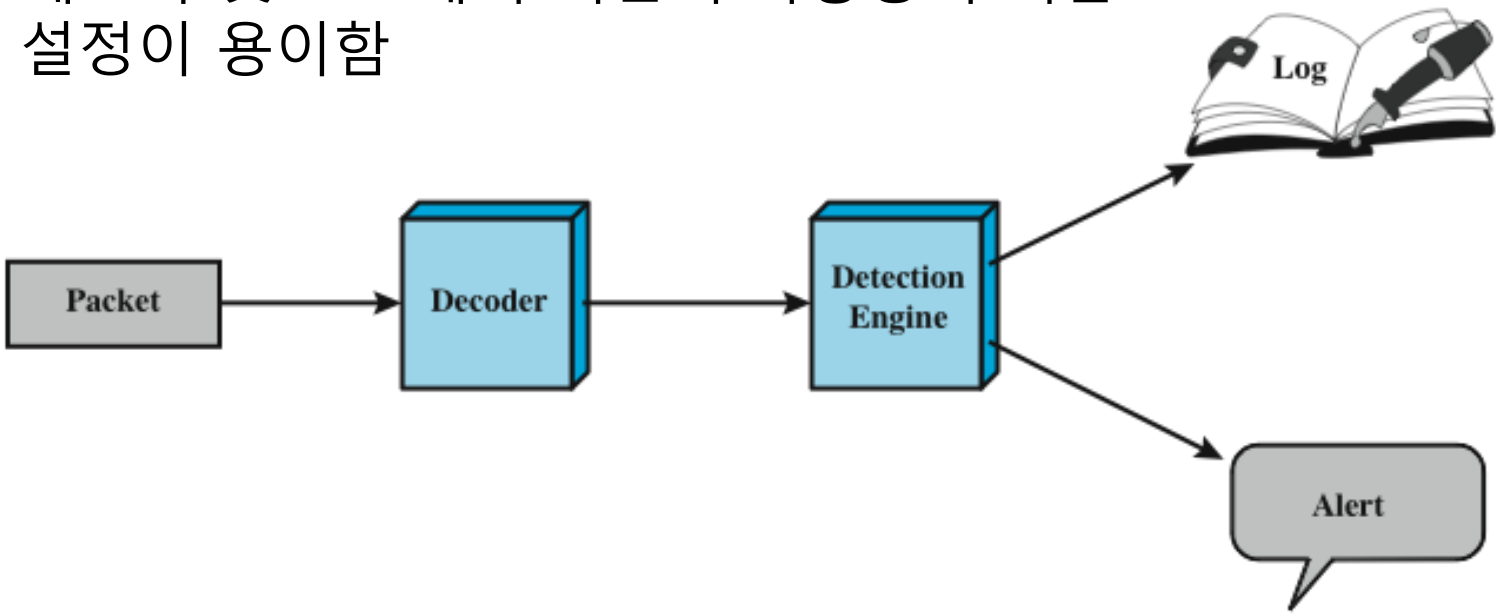


Figure 8.9 Snort Architecture

스노트 규칙

- 간단하고 유연성 있는 규칙 정의 언어를 사용함
- 각 규칙은 고정된 헤더와 많은 옵션들로 구성됨

Action	Description
Alert	지정된 경고 방법으로 경고를 생성한 후 패킷을 기록한다.
Log	패킷을 기록한다.
Pass	패킷을 무시한다.
Activate	경고한 후 또다른 동적 규칙을 활성화 시킨다.
Dynamic	활성화 된 규칙에 의해 활성화가 될 때까지 비활성화 되어 있다가 활성화가 되면 기록 규칙으로 작동한다.
Drop	iptable이 패킷을 버리고 패킷을 기록하도록 한다.
Reject	Iptable이 패킷을 버리고 기록한 후 TCP의 경우 TCP reset을 보내고 UDP인 경우 ICMP port unreachable 메시지를 보낸다.
sdrop	iptable이 패킷을 버리고 기록은 하지 않는다.

스노트 규칙 옵션의 예제

Meta-data	
msg	패킷이 이벤트를 발생시킬 때 보낼 메시지를 정의한다.
reference	추가적 정보를 얻기 위해서 연결할 외부 공격감지시스템을 정의한다.
classtype	패킷이 시도하고 있는 공격의 종류를 표시한다.
payload	
content	Snort가 패킷의 payload에서 특정 내용(텍스트나 바이너리)을 case-sensitive하게 검색할 수 있도록 한다.
depth	패킷 내 어느정도 깊이 까지 Snort가 특정 패턴을 검색해야 하는지를 정의한다. Depth키워드는 앞서 나온 content키워드를 수정한다.
offset	패킷 안에서 어디서부터 시작해서 패턴을 검색해야 하는 지를 지정한다. Offset은 앞서 나온 content 키워드를 수정한다.
nocase	Snort가 패턴을 검색하되 case는 무시한다. Nocase는 이전에 나온 content 키워드를 수정한다.
non-payload	
ttl	IP time-to-live 값을 검사한다. 이 옵션은 traceroute 시도를 감지하기 위해서 사용된다.
id	IP ID필드의 특정 값을 체크한다. 어떤 툴들은(exploits, scanners등 특이한 프로그램들) 이 필드를 여러가지 용도로 사용한다. 예를 들어 31337값이 해커들이 많이 사용하는 값이다.
dsize	패킷 payload크기를 터스트한다. 이는 비정상적인 패킷 사이즈를 검사할 때 사용된다. 많은 경우에 buffer overflow를 감지하는 데 사용된다.
flags	TCP 플래그의 특정 값을 찾는다.
seq	특정 TCP header 일련번호를 찾는다.
icmp-id	특정 ICMP ID 값을 찾는다. 어떤 비밀 통신 프로그램은 통신을 위해서 static ICMP 필드를 사용하기 때문에 유용할 수 있다. 이 옵션은 stacheldraht DDoS공격을 감지하기 위해서 개발됐다.
post-detection	
logto	규칙과 매칭되는 패킷을 특정 파일 이름으로 기록한다.
session	TCP세션으로부터 사용자 데이터를 추출한다. 많은 경우에 사용자가 telnet, rlogin, ftp, 웹세션에서 어떤 내용을 입력하는지가 매우 유용하다.