Chap 8.
Intrusion Detection

연세대학교

Examples of Intrusion

- 원격 관리자 권한 획득
- 웹 서버 조작
- 패스워드 추측/크래킹
- 신호카드번호가 포함된 데이터베이스 복사
- 허가 없이 개인 정보 보기
- 패킷 스니퍼(sniffer) 실행 - 모니터링
- 불법복제(해적판) 소프트웨어 배포
- 보안이 미비한 modem을 사용하여 내부 네트워크 접근
- 회사임원을 사칭하여 정보 획득
- 허가 없이 로그인 되어 있는 빈 workstation 사용

연세대학교

Intruder Behavior

공격대상 포착 및 정보 수집	초기 접속	권한 상승
정보 수집 및 시스템 공격	접근 관리	추적 회피

연세대학교

Hacker Patterns of Behavior

1. **select the target using IP lookup tools such as NSLookup, Dig, and others**
2. **map network for accessible services using tools such as NMAP (port scan)**
3. **identify potentially vulnerable services (in this case, pcAnywhere)**
4. **brute force (guess) pcAnywhere password**
5. **install remote administration tool called DameWare**
6. **wait for administrator to log on and capture his password**
7. **use that password to access remainder of network**

연세대학교

Criminal Enterprise Patterns of Behavior

신속하고, 정확하게 행동하여 자신의 동작을 탐지하기 어렵게 만듦

취약한 포트를 경유하여 경계(perimeter)을 공격함

트로이 목마(hidden software)를 사용하여 재진입을 위한 back-door를 남겨둠

sniffers를 사용하여 password들을 캡쳐함

노출될 때까지 옆에서 기다리지(stick around) 않음

연세대학교

Internal Threat Patterns of Behavior

자신과 친구들의 네트워크 계정 만들기 → 일상적으로 사용하지 않는 계정과 응용 프로그램에 접근 → 이전 또는 예상되는 고용주에게 email 보냄 → 은밀한 인스턴트 메시징 수행 → 불만이 있는 직원에게 영합하기 위해 웹사이트 방문 → 많은 수의 다운로드와 파일 복사를 수행 → 근무 외 시간에 네트워크 접근

연세대학교

Intrusion Detection Systems (IDSs)

- host-based IDS
  - 하나의 호스트의 특성과 이벤트를 감시하여 의심스러운 활동을 감지함.
- network-based IDS
  - 네트워크 트래픽을 감시하고 네트워크, 전송 및 응용 프로그램 프로토콜을 분석하여 의심스러운 활동을 식별함.
- Distributed or hybrid IDS
  - 중앙 분석기에서 센서들, 호스트, 네트워크 IDS에서 오는 정보들을 잘 결합하여 침입 활동을 더 잘 식별하고 대응함.

연세대학교

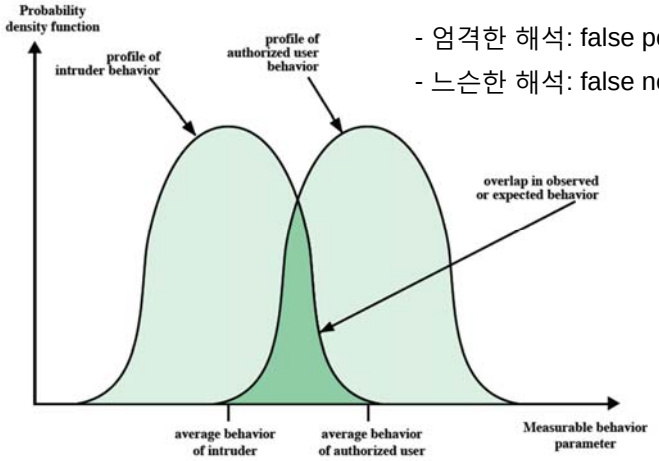
Intrusion Detection Systems (IDSs)

- IDS의 논리적 구성 요소
  - Sensors
    - 데이터 수집
  - analyzers
    - 침입이 발생 했는 지 여부를 결정
  - user interface
    - 출력을 보거나, 시스템 행동을 제어

연세대학교

IDS Principles

- 침입탐지 시스템의 원리
  - 침입자의 행동이 일반 사용자와는 다르다는 가정에 기반을 둠
- 침입자와 일반 사용자의 행동 특성이 겹칠 수 있음(overlap)



- 엄격한 해석: false positive
- 느슨한 해석: false negative

IDS Requirements

- 지속적으로 실행
- fault tolerant – 시스템 crash 후 재시작 했을 때에 복구 가능
- resist subversion – 자신을 감시하여 공격받으면 바로 탐지 가능
- 시스템에 최소한의 오버헤드 부과
- 시스템 보안 정책에 따라서 설정 가능
- 시스템과 사용자들의 행동 변화에 적응 가능
- 많은 수의 시스템을 감시할 수 있도록 확장 가능
- graceful degradation of service - 일부 구성요소가 중지되었을 때에 나머지 요소가 적게 영향 받으면서 동작 가능
- 재시작 없이 동적 재설정 가능

Analysis Approaches

이상 탐지(Anomaly detection)

- 일정 기간 동안 합법적인 사용자의 행동과 관련된 데이터 수집
- 현재 관찰된 행동을 분석하여 이 행동이 합법적인 사용자의 행동인지 또는 침입자의 행동인지 여부를 결정합니다

Signature/Heuristic detection

- 알려진 **악의적인 데이터 패턴 또는 공격 규칙**을 사용하여 현재 행동과 비교
- 오용(misuse) 탐지라고도 함
- 패턴이나 규칙이 있는 미리 알려진 공격만 식별 가능

Anomaly Detection

- 다양한 분류 방법이 사용됨

Statistical	Knowledge based	Machine-learning
• 관찰된 지표를 **단변량, 다변량 또는 시계열 모델** 등의 **통계적 분석**을 사용하여 동작을 분석	• 정상 동작을 모델링하는 일련의 규칙에 따라서 관찰된 동작을 분류하는 **expert system**을 사용	• data mining 기술을 사용하여 **학습된 데이터**로부터 관찰된 동작에 적합한 분류를 자동적으로 결정함 → **기계 학습**

Signature or Heuristic Detection

- Signature approaches
  - **signature** – 침입/공격이 의심되는 알려진 악성 데이터 패턴
  - 시스템 저장 데이터 또는 네트워크 전송 데이터에 대해 signature 집합의 패턴과 일치되는 지 비교
  - 오탐지율을 최소화하기 위해서 signature는 매우 커야 함
  - Anti-virus 제품, 네트워크 침입탐지 시스템(NIDS)에서 널리 사용되는 방식
  - zero day 공격에 취약함
- Rule-based heuristic identification
  - **규칙**(rule) – 침입/공격이 의심되는 행동을 정의함
  - **규칙**을 사용하여 알려진 취약점을 이용하는 공격과 침입을 식별함
  - (예) SNORT – rule-based NIDS

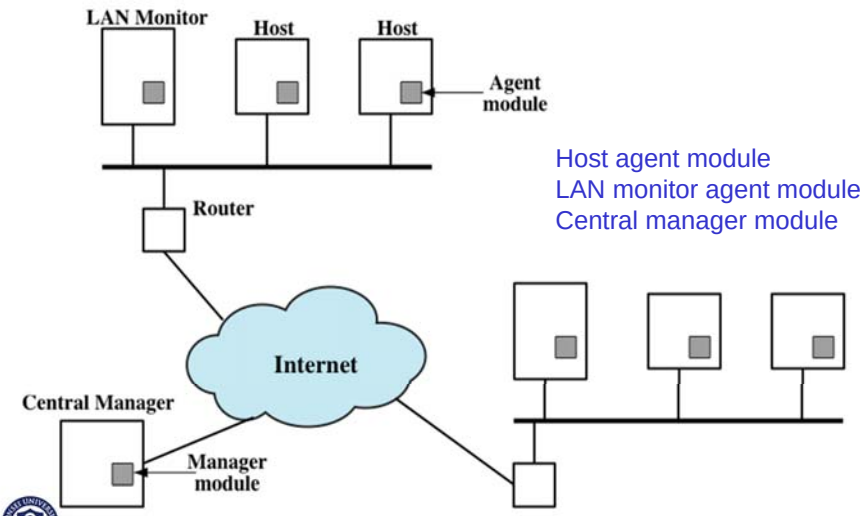
Host-Based IDS (HIDS)

- 공격에 취약한 시스템에 특별한 보안 소프트웨어 계층을 추가함
- 이상(anomaly), 서명(signature0 또는 경험적(heuristic) 접근 방법 사용 가능
- 의심스러운 동작을 탐지하기 위해 활동을 감시
  - 주 목적은 침입 탐지, 이벤트 기록(log), 경고 통지
  - 외부 침입과 내부 침입 모두 탐지

Data Sources and Sensors

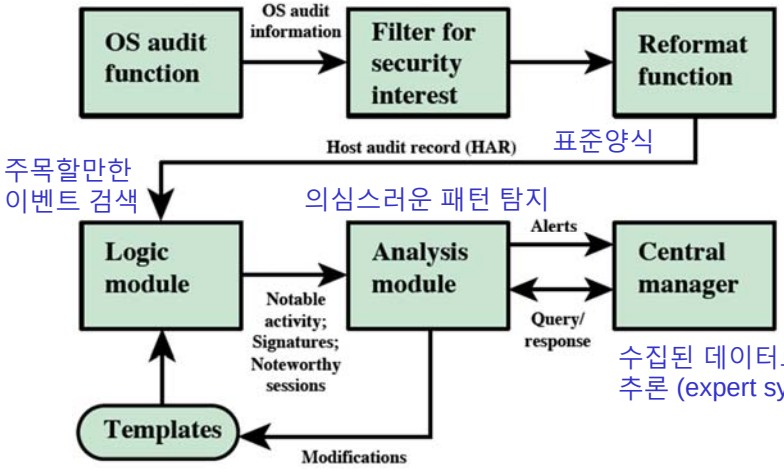
- Sensor
  - 데이터를 수집함
  - 침입 탐지에 기본적인 구성요소
- 일반적인 데이터 소스
  - system call 추적 (table 8.2 참고) – Unix/Linux OS에서 효과적
  - 감사(log 파일) 기록
  - 파일 무결성 검사 – checksum 생성 및 검사
  - registry 접근 감시 – windows OS only

Distributed Host-Based IDS



Host agent module
LAN monitor agent module
Central manager module

Agent Architecture

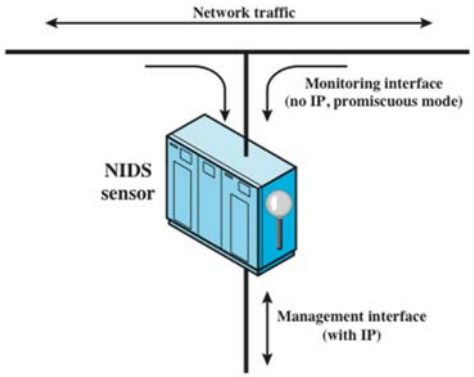


Network-Based IDS (NIDS)

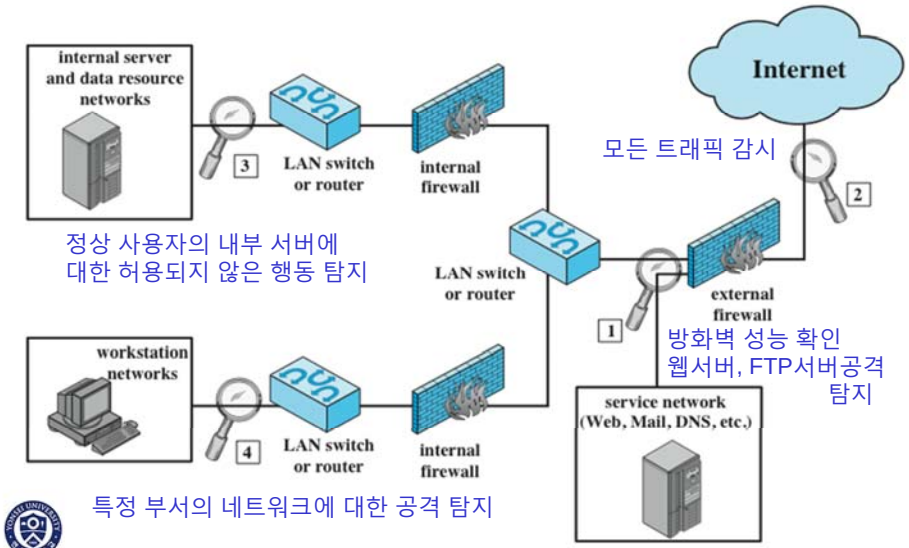
- 네트워크의 선택 지점에서 트래픽을 모니터링
- 실시간 또는 거의 실시간으로 패킷 단위로 트래픽을 검사
- 네트워크, 전송 또는 응용 계층 프로토콜 활동 분석 가능
- 다수의 센서, NIDS 관리용 서버, 관리자용 콘솔로 구성됨
- 트래픽 패턴 분석은 센서, 관리 서버 또는 둘의 조합에서 수행 가능

NIDS Sensor Deployment

- inline sensor
  - network segment에 삽입되어 센서를 통과하는 트래픽을 감시
- passive sensors
  - 네트워크 트래픽을 복사본을 감시



NISD Sensor Deployment Example



Intrusion Detection Techniques

- signature detection(misuse detection)에 적합한 공격
  - application, transport, network 계층에서의 프로토콜을 분석하여 이 프로토콜을 대상으로 한 공격을 탐지
  - unexpected application services, policy violations
- anomaly detection에 적합한 공격
  - denial of service attacks
  - scanning - 시스템의 특성과 취약점을 찾기 위한 포트 조사
  - worms – 평소에 통신을 하지 않았던 호스트와 사용하지 않았던 포트 번호 사용을 탐지. 많은 웜이 스캐닝을 수행함.

Stateful Protocol Analysis (SPA)

- 상태기반 프로토콜 분석
  - 관찰된 network traffic과 공급업체가 제공하는 protocol traffic에 대한 profile과 비교하여 비정상 동작을 탐지
  - network, transport, application 프로토콜 상태를 이해하고 추적하여 예상대로 진행되는지 확인함.
- 단점: 많은 자원을 사용함

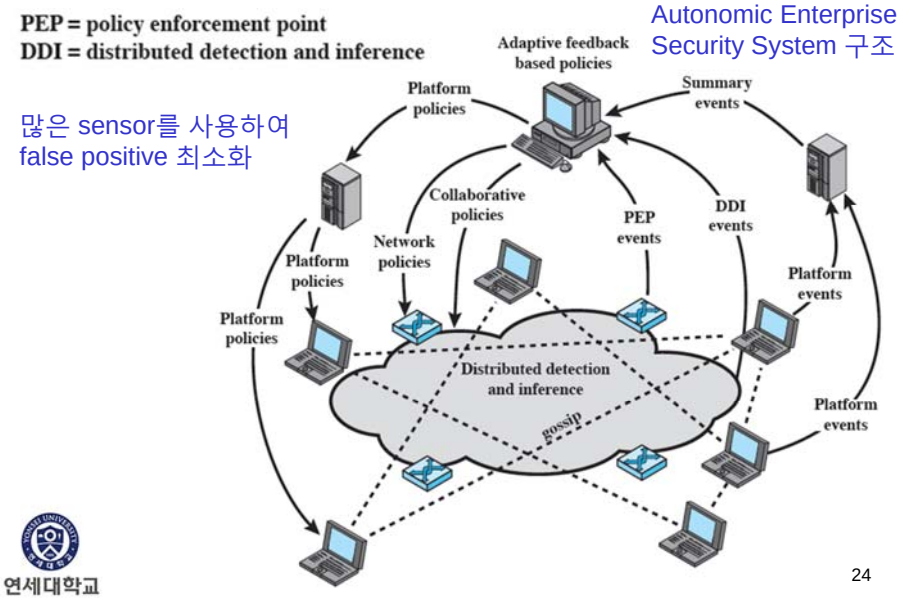
Logging of Alerts

- NIDS 센서가 기록하는 전형적인 정보
  - Timestamp
  - Connection or session ID
  - Event or alert type
  - Rating(점수-우선순위, 심각도, 영향력, 신뢰도)
  - Network, transport, and application layer protocols
  - Source and destination IP addresses
  - Source and destination TCP or UDP ports, or ICMP types and codes
  - Number of bytes transmitted over the connection
  - Decoded payload data (application requests and responses)
  - State-related information (인증된 사용자이름 등)

Distributed or Hybrid Intrusion Detection

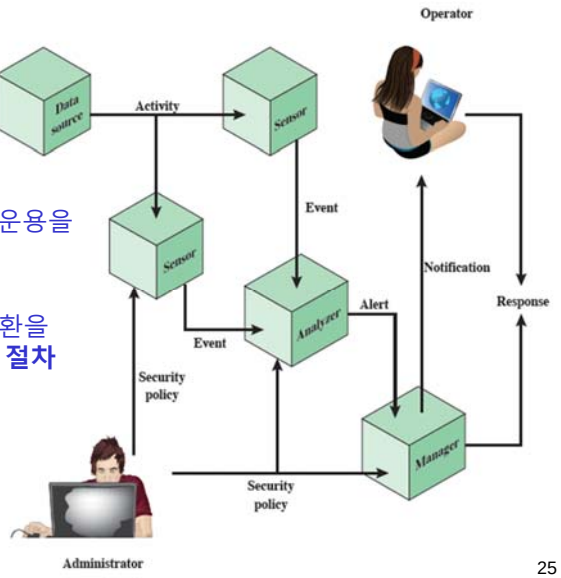
Autonomic Enterprise Security System 구조

많은 sensor를 사용하여 false positive 최소화



Intrusion Detection Exchange Format

- 분산 IDS에서 상호 운용을 위한 표준이 필요
- 침입탐지 메시지 교환을 위한 **데이터 형식**과 **절차** 등이 정의됨

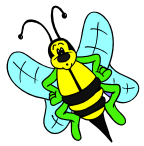


Honeypot

- 하니팟 – 공격자들을 중요시스템으로 부터 멀리로 유인하기 위해 설계된 미끼 시스템(decoy systems)
  - 공격자가 중요 시스템에 접근 하지 못하도록 유인함
  - 공격자 활동에 대한 정보 수집
  - 관리자가 대응할 수 있을 만큼 오랫동안 공격자가 시스템에 머물게 유도함
- 정상 사용자가 접근하지 않을 가공의 정보로 채워짐
- honeypot의 자원은 실제적인 가치를 갖지 않음
  - 수신 통신은 probe, scan, attack일 가능성이 높음
  - 송신 통신은 시스템이 이미 침입되었을 가능성을 나타냄
- 해커가 네트워크 내에 있으면 관리자는 이들의 행동을 관찰하여 방어를 고안할 수 있음

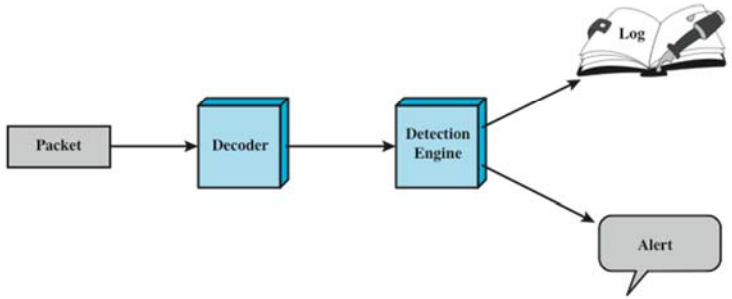
Honeypot Deployment

- 방화벽 외부
- 외부 접근이 가능한 방화벽 내부 (DMZ)
- 방화벽 내부



SNORT

- lightweight IDS
  - real-time packet capture and rule analysis
  - easily deployed on nodes
  - uses small amount of memory and processor time
  - easily configured



Snort Rule Formats

- 형식
  - action, protocol, src IP, src port, direction, dest IP, dest port, option-keyword, option-arguments …
- alert tcp $EXTERNAL_NET any -> 192.168.3.0/24 80 (msg:"Sample alert"; content:"http|3a|//www.vorant.com/test.cgi?id=pwn3d"; nocase; offset:12; classtype: web-application-activity; reference:url,http://www.vorant.com/advisories/20060405.html; sid:2000123; rev:1;)

- alert tcp $EXTERNAL_NET any -> 192.168.3.0/24 80 (msg:"Sample alert"; pcre:"/GET.*\.htm/i"; classtype: webapplication-activity; reference:url,http://www.vorant.com/advisories/20060405.html; sid:2000123; rev:1;)

SNORT Rules

- use a simple, flexible rule definition language
- each rule consists of a fixed header and zero or more options

Action	Description
alert	Generate an alert using the selected alert method, and then log the packet.
log	Log the packet.
pass	Ignore the packet.
activate	Alert and then turn on another dynamic rule.
dynamic	Remain idle until activated by an activate rule , then act as a log rule.
drop	Make iptables drop the packet and log the packet.
reject	Make iptables drop the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
sdrop	Make iptables drop the packet but does not log it.