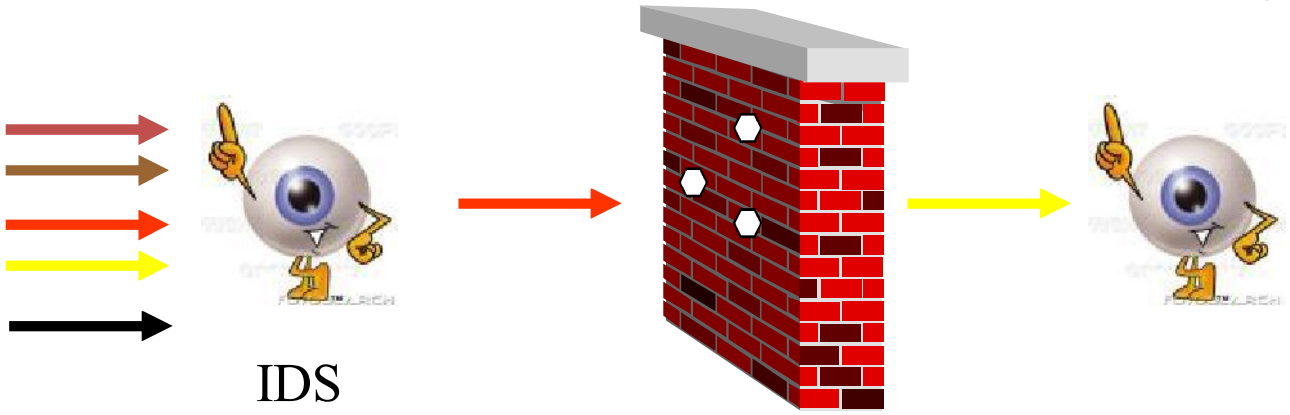
سیستم تشخیص نفوذ
Intrusion Detection System (IDS)

IDS چیست؟

- تعریف Intrusion
  - مجموعه فعالیت هائی که برای مخدوش کردن Integrity، confidentiality یا قابلیت دسترسی منابع شبکه انجام می شود.
- تشخیص نفوذ:
  - فرآیند شناسایی و مقابله با فعالیت های بدخواهانه ای است که منابع شبکه و محاسباتی را هدف قرار داده اند.

ضرورت IDS

- فایروال به تنهائی قادربه فیلتر کردن تمامی اعمـال خرابکارانـه نیست. به عنوان مثال نمی توانـد پـورت ۸۰ یـک سـرور وب را ببندد.



IDS

- فرضیات اولیه:
  - فعالیت های سیستم قابل مشاهده هستند.
  - فعالیت های نرمال و بدخواهانه دارای نشانه های مشخصی هستند.
- مؤلفه ها:
  - از دیدگاه الگوریتمی
    - ویژگی ها: به دست آوردن نشانه های نفوذ از داده ها
    - مدل ها: کنار هم قرار دادن نشانه ها و شناسایی حمله

کاربرد IDS

- جلوگیری از نفوذ

  مثال۱:

  – شناسایی سرریز بافر و حذف آن

  – استفاده از فایروال برای فیلتر کردن ترافیک بدخواهانه

  – مثال ۲: شناسائی حملات DOS

- شناسایی نفوذ زمانی صورت می گیرد که جلوگیری از نفـوذ کـارایی نداشته باشد.

  – شناسایی حملات در حال اجرا

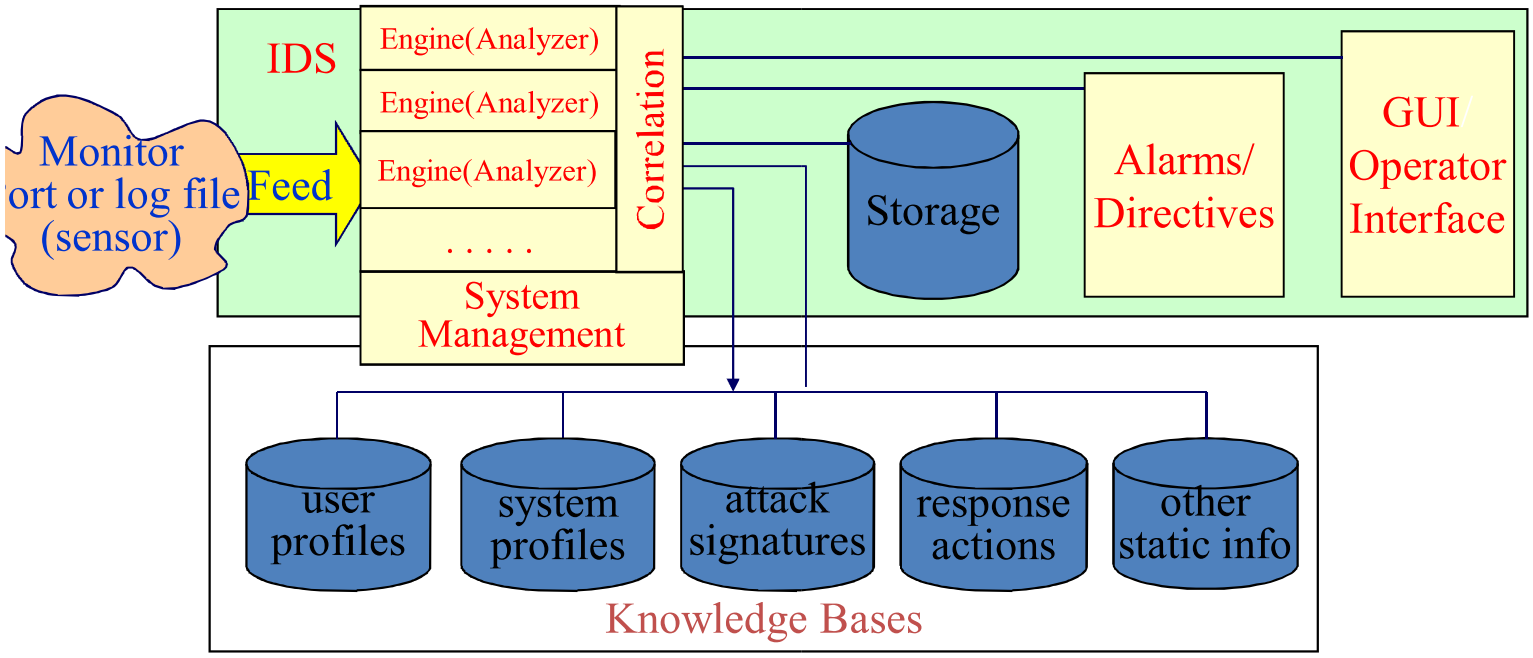
    - الگوی ترافیک شبکه، فراخوانی های سیستمی مشکوک

  – کشف تغییرات سیستم

نمونه هائی از موارد قابل شناسایی

- نفوذهای موفقیت آمیز و در حال انجام
- حملات توسط کاربران قانونی
  - استفاده غیر قانونی از حق دسترسی مدیر سیستم
  - دسترسی غیر نامعتبر به داده و منابع
- تروجان ها
- ویروس ها و کرم های اینترنتی
- حملات DDoS

معماری IDS



User/System Profile-

-پروفایل رفتاری نرمال و غیر نرمال کاربران و سیستم ها

-امضا های حملات

-یک الگو از محتوی بسته ها یا الگوی رفتاری از یک حمله یا نفوذ

-مجموعه رفتارهائی که باید در مقابل حملات انجام شود

انواع روش های شناسایی

- مبتنی بر امضاء (Signature-based)
  - Misuse Detection
  - شناسایی الگو (Pattern Matching)
  - مبتنی بر قانون (Rule-based)
- مبتنی بر ناهنجاری (Anomaly-based)
  - Behavior-based Detection
    - سطح کاربرد (Application-level)
    - سطح کاربر (User-level)
    - سطح سیستم عامل (OS-level)
    - سطح شبکه (Network-level)
- مبتنی بر مشخصات (Specification-based)

روش مقایسه دو رو شها

- False Positive
  - یک فعالیت به عنوان حمله شناسائی شده است در حالی کـه حملـه نیست.
- False Negative
  - فعالیت خرابکارانه شناسائی نشده است.
- با استفاده از Data Set های برچسب زده شده می توان میزان FP و FN رامقایسه کرد.

شناسایی مبتنی بر امضاء

- IDSهای مبتنی بر امضاء رویدادها را با الگوهایی که بدخواه معرفی شده اند، مقایسه می کنند.
- این سیستم ها، دارای پایگاه داده ای هستند که حاوی اطلاعاتی در مورد امضاء حملات و آسیب پذیری های سیستمی است و از این پایگاه داده استفاده می کنند تا نفوذ ها و حملات را تشخیص دهند.
  - دنباله ای از بایت ها
  - نوع پروتکل
  - شماره پورت

شناسایی مبتنی بر امضاء

- دارای False Positive پایین
  – معلوم است که چه چیزی مشکوک و چه چیزی نرمال است.
- فقط قادر به شناسایی رفتارهایی است که قبلاً بـه عنـوان رفتـار مشکوک معرفی شده اند.
- ساده و کارا است.
- امضاءهای آن قابل به اشتراک گذاری است.

امضاء (Signature)

- امضاء یک الگو یا مجموعه ای از قوانینی است که می تواند یک حمله را مشخص کند.
- امضاءها با توجه به حملات و آسیب پذیری های شناخته شده ساخته می شوند.
- امضاءها مستقل از الگوهای رفتاری کاربران، سیستم و شبکه نوشته می شوند.

مثال: Trinoo

- بدافزاری برای اجرای حملات DDoS
- موقعی که کلاینت Trinoo روی هاست نصب شد، روی یکی از پورت های UDP گوش می کند.
- Master پیغام png به کلاینت هایش می فرستد و کلاینت ها پیغام PONG را به پورت 31335/UDP ارسال می کنند.

Trinoo امضاء

Trin00
http://www.snort.org/snort-db/sid.html?sid=223

GEN:SID	1:223
Message	DDOS Trin00 Daemon to Master PONG message detected
Rule	alert udp $EXTERNAL_NET any -> $HOME_NET 31335 (msg:"DDOS Trin00 Daemon to Master PONG message detected"; content:"PONG"; reference:arachnids,187; classtype:attempted-recon; sid:223; rev:3;)

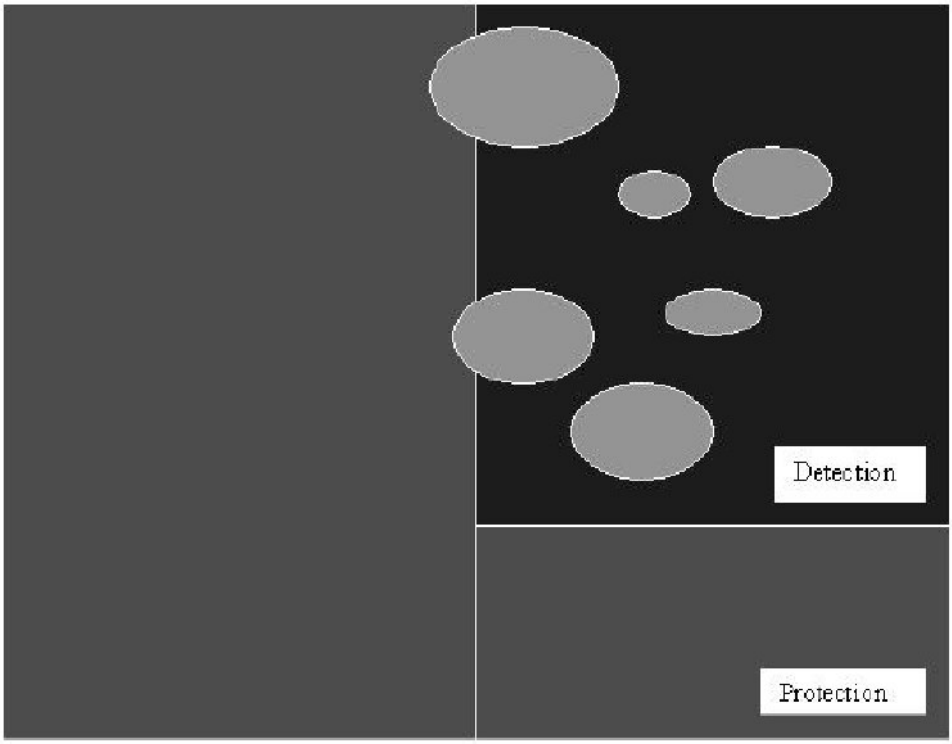
شناسایی مبتنی بر امضاء

- سیستم های مبتنی بر امضاء دارای یک فاز یادگیری هستند.
  - عملیات زمانبری برای شناسایی و تولید امضاء حملات جدید
  - احتیاج به دانش فرد خبره
  - عدم شناسایی حملات جدید بدون داشتن امضاء آنها
- False Negatives
  - عدم شناسایی حملات جدید و تغییر یافته
- False Positives
  - امضاءهای ضعیف باعث شناسایی رویدادهای نرمال به عنوان نفوذ می شوند.

استخراج امضاء

- استفاده از خصوصیات ثابت حملات شناخته شده
  - محتوای ویروس ها و کرم های شناخته شده
  - شماره پورت برنامه های دارای سرریز بافر شناخته شده
  - عدم شناسایی در صورت تغییر
    - کرم های چند ریختی: هر کپی دارای محتوای متفاوتی است.
- استخراج سریع و خودکار امضاء حملات جدید
- استفاده از Honeypot برای استخراج امضاء

شناسایی مبتنی بر امضاء

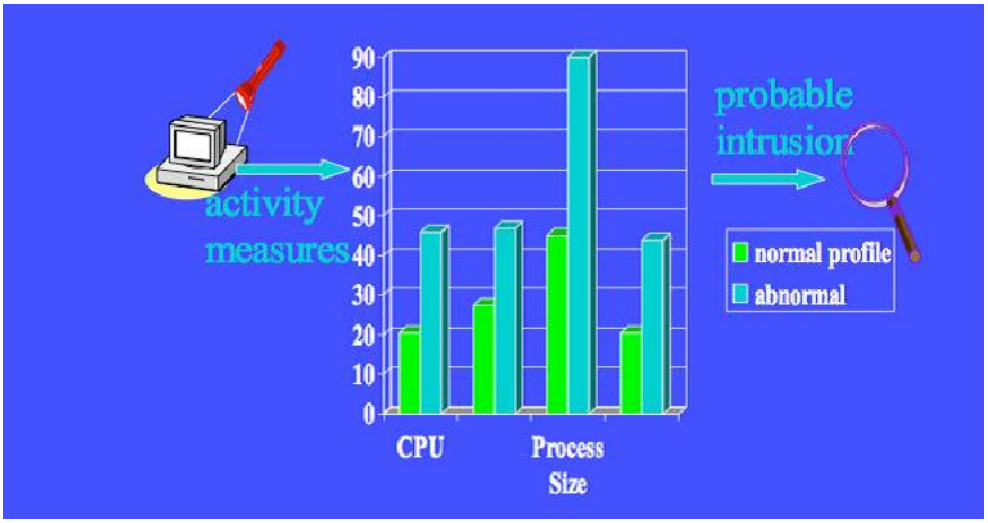


شناسایی مبتنی بر ناهنجاری

- IDSهای مبتنی بر ناهنجاری رویدادها را با الگوهایی که رفتار نرمال و قابل قبول معرفی شده اند، مقایسه می کنند.
- رفتار غیر عادی به رفتاری گفته می شود که به طور چشمگیری با رفتاری که معمولاً مشاهده می شود، متفاوت باشد.
  - انحراف از الگوهای رفتاری یاد گرفته شده
- فرض این روش بر این است که استفاده های بدخواهانه باعث ایجاد رفتارهایی متفاوت از رفتار نرمال سیستم می شوند.

شناسایی مبتنی بر ناهنجاری

- سیستم های شناسایی مبتنی بر ناهنجاری، پروفایلی کاری برای تمام کاربران، پروسس ها و شبکه تهیه می کنند که نشان دهنده الگوی رفتاری نرمال آن ها است. هر انحرافی از این پروفایل به عنوان نفوذ تشخیص داده می شوند.



شناسایی ناهنجاری

- پروفایل نشان دهنده رفتار نرمال است.
  - برای سیستم های کوچک عملیاتی است.
- پروفایل معمولاً آماری است.
  - به صورت دستی ساخته شود (خیلی سخت است).
  - استفاده از تکنیک های یادگیری ماشین و داده کاوی
    - ثبت فعالیت های سیستم و آموزش IDS برای شناسایی الگوهای نرمال
  - ریسک: مهاجم می تواند حملاتش را انجام دهد تا IDS آنها را به عنوان فعالیت های نرمال بشناسد. (Data Drift)
    - پورت اسکن های با نرخ پایین

پروفایل

- پروفایل مدل های استفاده ای است که توسط شاخص هایی مربـوط به سیستم و شبکه تهیه می شوند.
  - فعالیت سیستم و شبکه در یک بازه زمانی
  - فعالیت های ورود (Login) کاربر
    - تعداد و زمان های ورود، مکان های ورود، آخرین ورود، تعداد اشتباه وارد کردن رمز عبور
  - دستورات و برنامه های اجرا شده
    - تواتر اجرا، میزان منابع مصرف شده (CPU، I/O، حافظه)، اجراهای ناموفق
  - فعالیت های دسترسی به فایل
    - تـواتر عملیـات خوانـدن/نوشـتن/سـاختن/حـذف کـردن، ثبـت خوانـدن/نوشـتن، خواندن/نوشتن/ساختن/حذف کردن نا موفق

شناسایی مبتنی بر ناهنجاری

- ایده کلی: "رفتار غیر عادی" = "مشکوک"
- یادگیری خودکار رفتار نرمال
- شناسایی حملات جدید و انواع تغییر یافته آن ها
- بدون مراقبت خبره قابل اجرا است.
- رفتار نرمال باید تعریف شود.
- تولید هشدار اشتباه
  - رفتار غیر عادی لزوماً بدخواهانه نیست.
  - رفتار عادی لزوماً بی خطر نیست.
- حجم پردازشی بالا

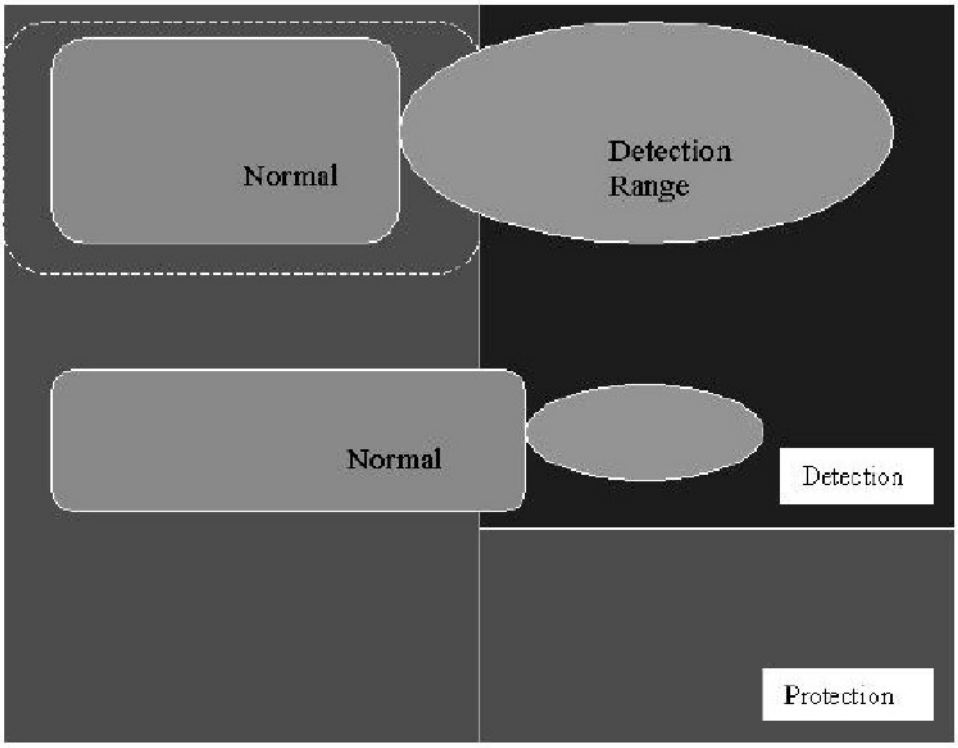
False Negatives

- تمام جنبه های رفتارهای نرمال قابل شناسایی نیست.
  - سیستم ها پیچیده هستند و نمی توان تمام ابعاد آنرا در نظر گرفت.
  - انحراف از رفتار نرمال شناخته نشده، قابل شناسایی نیست.
- فعالیت های خرابکارانه در فاز یادگیری صورت گیرد.
  - سیستم فعالیت های خرابکارانه را به عنوان رفتار نرمال در نظر می گیرد و آن را شناسایی نمی کند.
- اصل فرض لزوماً صحیح نیست.
  - رفتار عادی لزوماً بی خطر نیست.

False Positives

- مهمترین دلیل نرخ False Positive بالا، عدم وجود داده بردارنده تمام رفتارهای نرمال است تا از آن برای یادگیری استفاده شود.
- اصل فرض لزوماً صحیح نیست.
  - رفتار غیر عادی لزوماً نشاندهنده نفوذ نیست.
  - فاکتورهای دیگری مانند ارائه سرویس جدید وجود دارند که باعث ایجاد تغییر در رفتار نرمال می شوند.

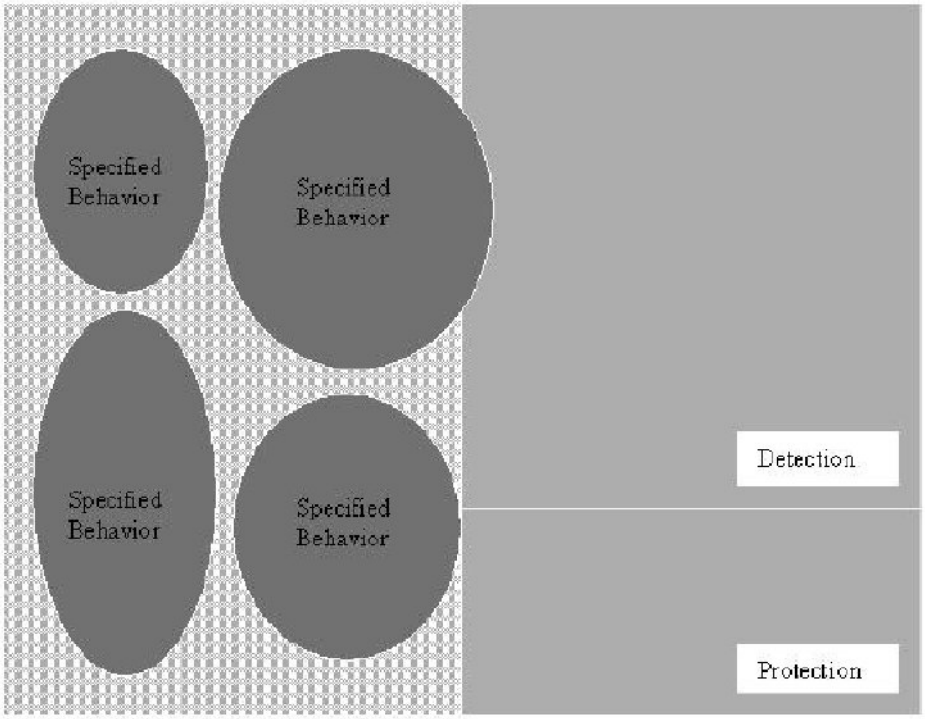
شناسایی مبتنی بر ناهنجاری



شناسایی مبتنی بر خصوصیات

- حالت خاصی از شناسایی مبتنی بر امضاء
- این سیستم ها شامل امضاءهای رفتار نرمال هستند.
- هر رویدادی که از این امضاءها انحراف داشته باشد، به عنوان نفوذ تشخیص داده می شود.
- این سیستم ها رفتارهایی که برای آن ها تعریف نشده را به عنوان نفود تشخیص می دهند.

شناسایی مبتنی بر مشخصات



انواع IDS از دیدگاه کاربری

- مبتنی بر هاست (Host-based)
  - HIDS
  - فعالیت های یک هاست را مانیتور می کند.
  - مزایا: دید کاملی روی رفتار برنامه های در حال اجرا روی هاست دارد.
- مبتنی بر شبکه (Network-based)
  - NIDS
  - معمولاً روی روتر یا فایروال نصب می شود.
  - ترافیک شبکه را مانیتور می کند و سربار و محتویات بسته ها را بررسی می کند.
  - مزایا: توانایی محافظت از تعداد زیادی هاست را دارد و می تواند حملات global را بهتر تشخیص دهد.

IDS مبتنی بر هاست

- با مانیتور کردن اتفاقاتی که در سیستم عامل می افتد، برنامه هایی که مورد حمله قرار گرفته اند را شناسایی می کند.
  - ثبت کردن تمام رویدادهای سیستمی (دسترسی به فایل، ...)
  - مانیتور کردن اجرای دستورات شل و فراخوان های سیستمی توسط کاربران و برنامه ها
- معایب
  - به ازای هر هاست یک HIDS لازم است.
  - اگر مهاجم هاست را در اختیار بگیرد با دستکاری سیستم می تواند مانع از شناسایی حملات شود.
  - دید IDS محدود به همان هاست بوده و قادر به شناسایی حملات global نمی باشد.

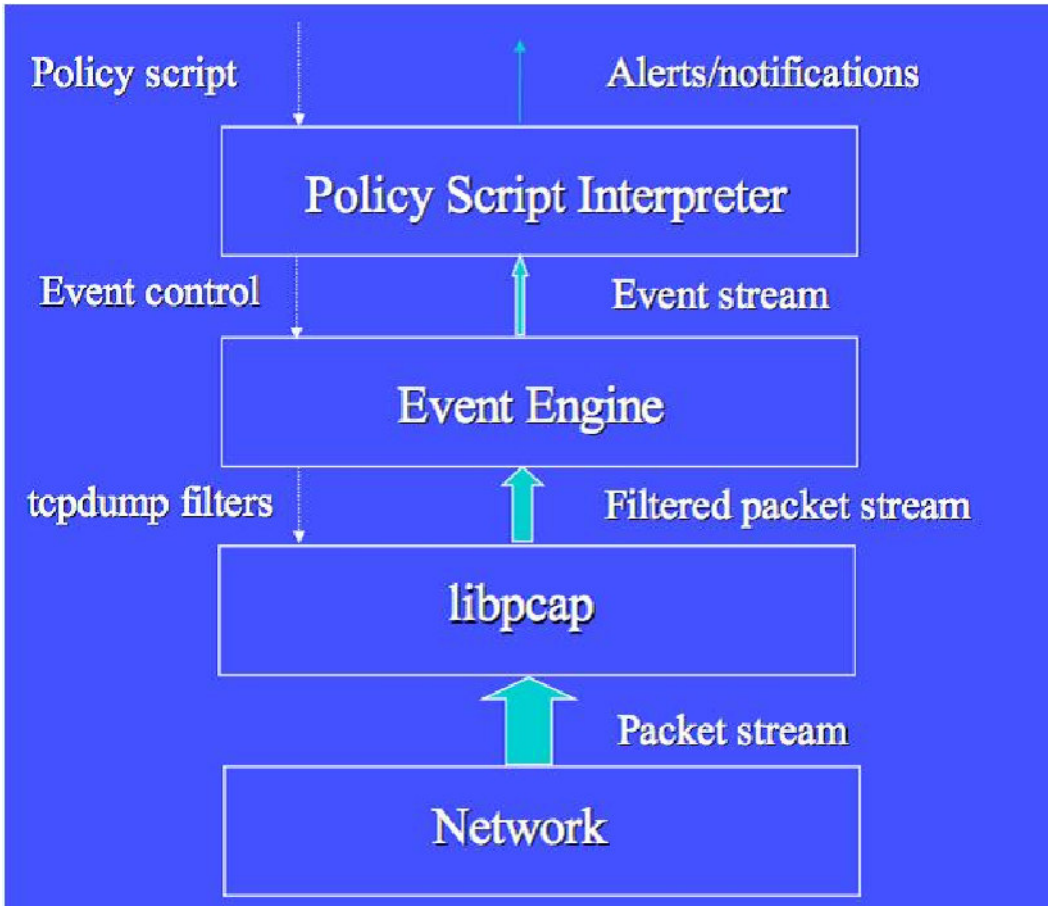
رویدادهای قابل مانیتور هاست ها

- فراخوان های سیستمی (OS System Calls)
- دستورات shell
- ترافیک شبکه هاست
- پروسس ها
- کلید های فشار داده شده
- دسترسی های به فایل ها و دیوایس ها

IDS مبتنی بر شبکه

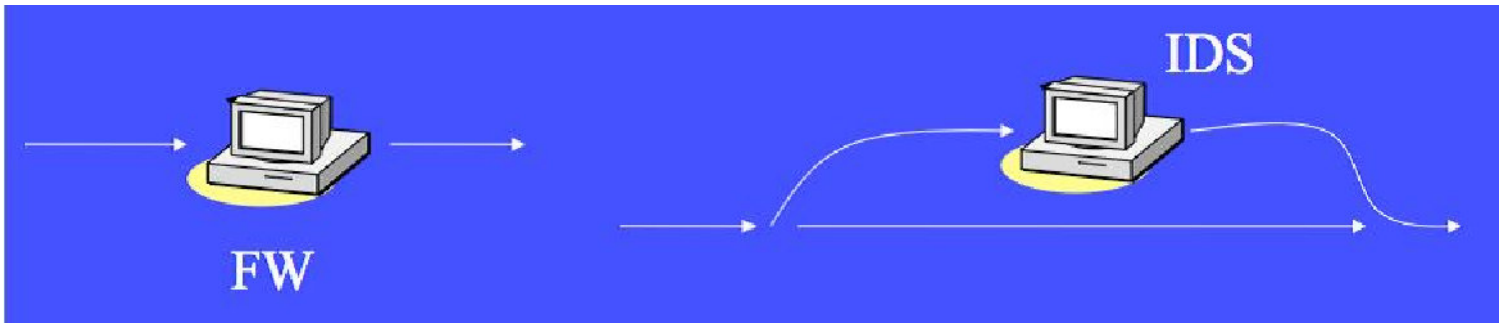
- بررسی ترافیک شبکه
  - استراق سمع ترافیک عبوری از روتر
  - منفعل (Passive): بر خلاف فایروال
- شناسایی نقض های ایجاد شده در پروتکل ها، الگوهای غیر معمول ارتباطات و امضا حملات در محتویات بسته ها
- معایب
  - عدم توانایی بررسی ترافیک های رمز شده (IPsec، VPN)
  - تمام حملات فقط با بررسی ترافیک شبکه، قابل شناسایی نیستند.
  - بررسی و پردازش حجم زیادی از ترافیک شبکه

معماری IDS مبتنی بر شبکه



مقایسه فایروال و NIDS

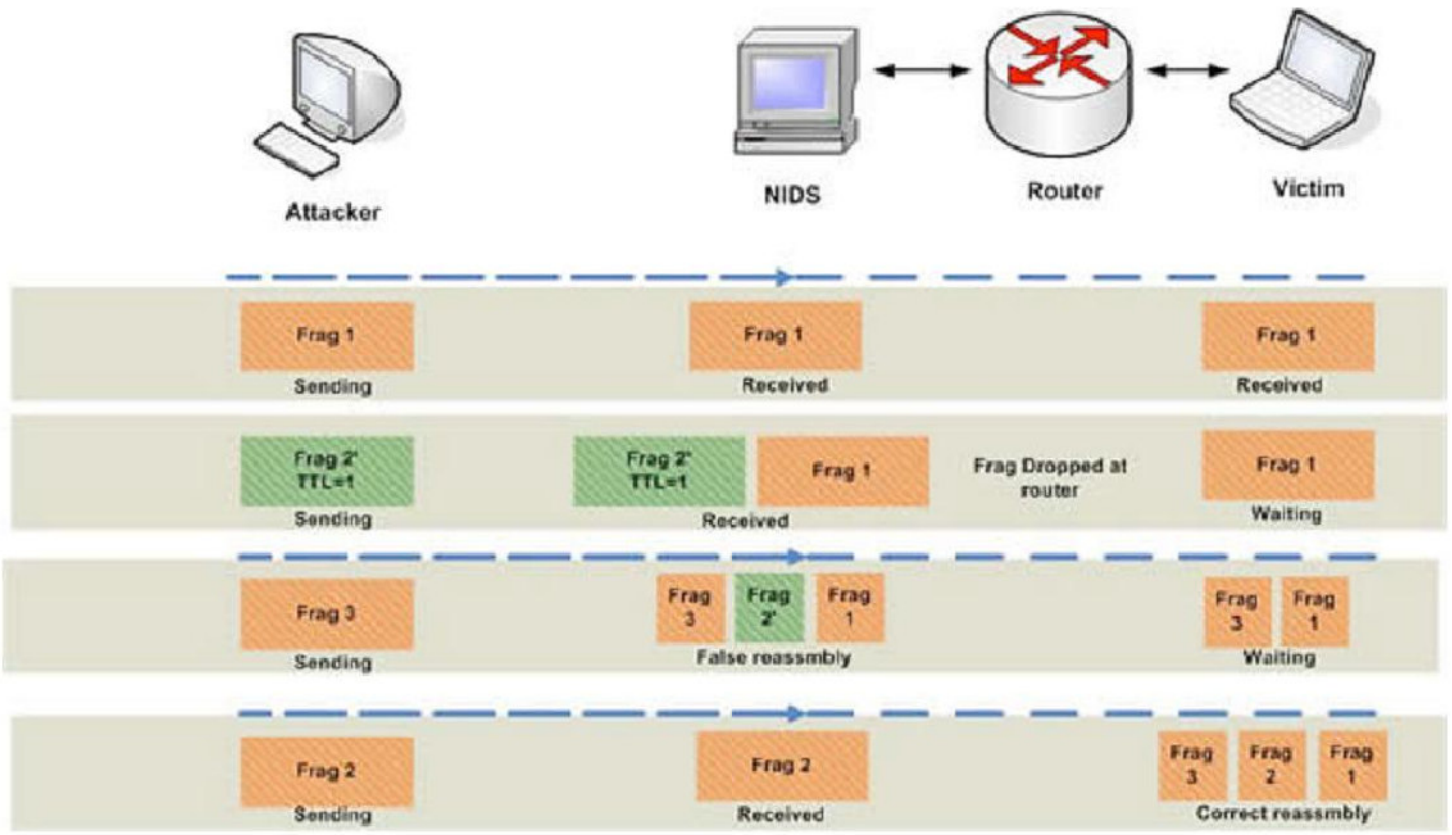
- فایروال
  - فیلترینگ فعال (Active Filtering)
- NIDS
  - مانیتورینگ منفعل (Passive Monitoring)



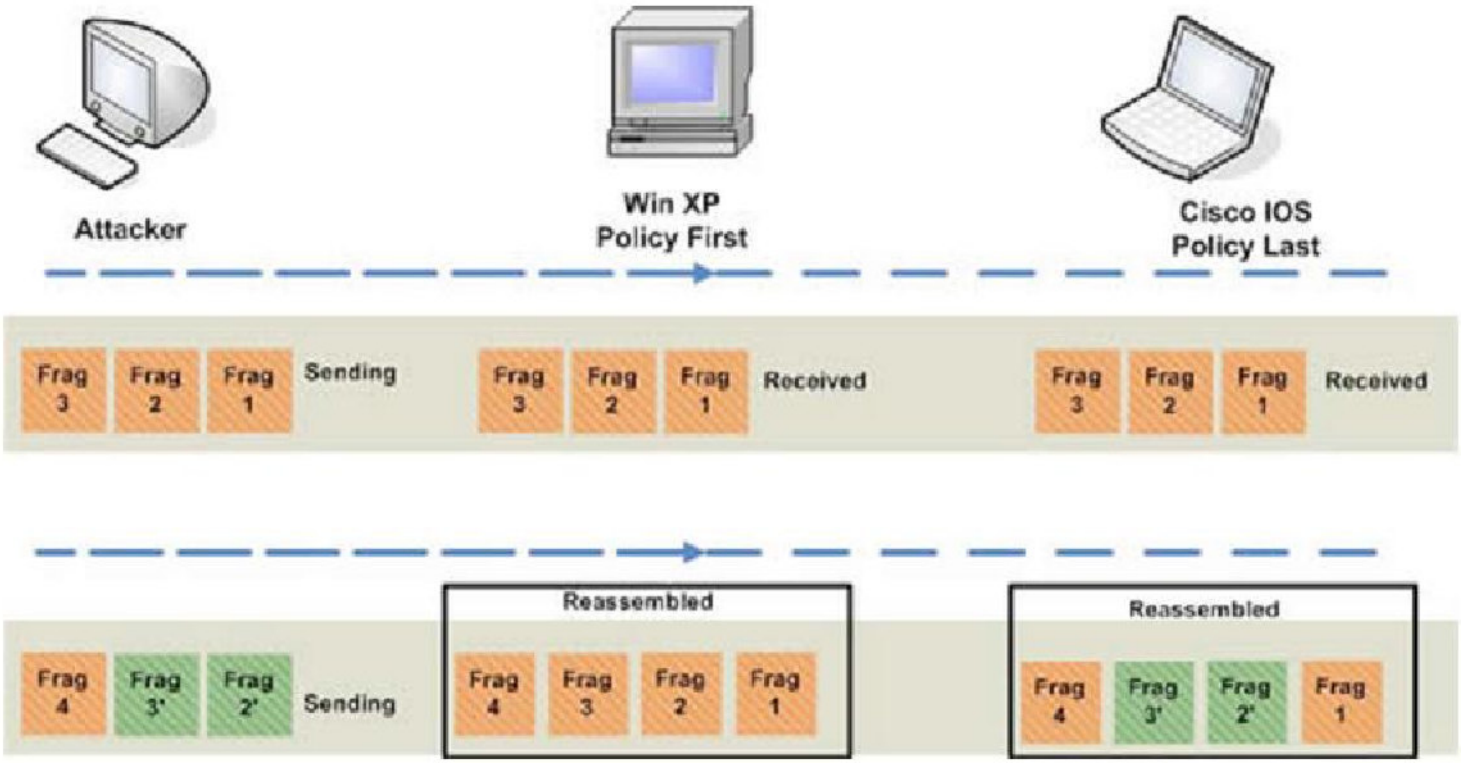
گول زدن NIDS

- چیزی که NIDS می بیند لزوماً چیزی نیست که هاست دریافت می کند.
  - حملات Insertion/Evasion
    - NIDS باید عملیات دوباره بازسازی بسته ها را به طور کامل انجام دهد.
  - اما همچنان ابهاماتی در پروتکل ها و سیستم عامل ها وجود دارد:
    - TTL
    - Fragments

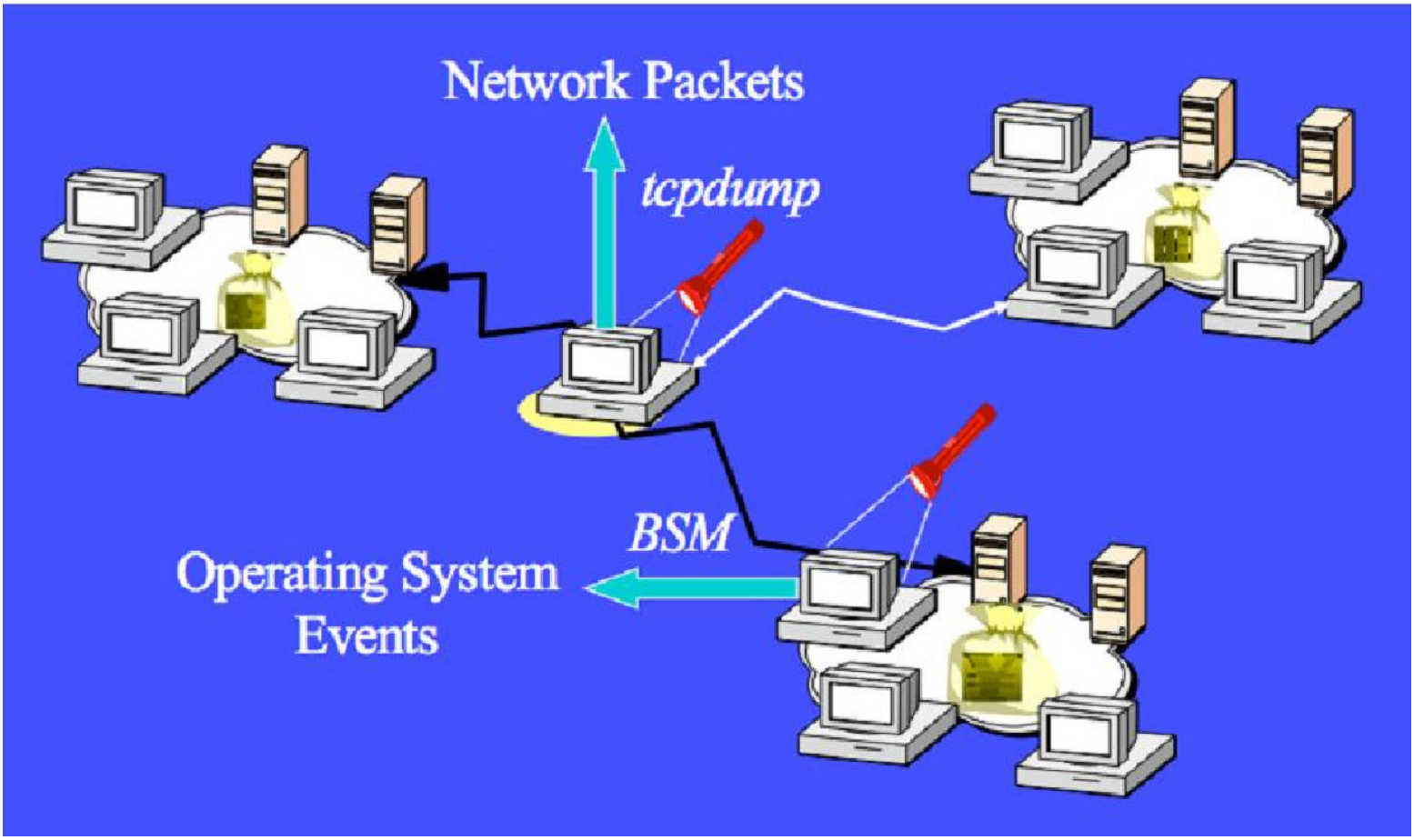
Insertion حمله



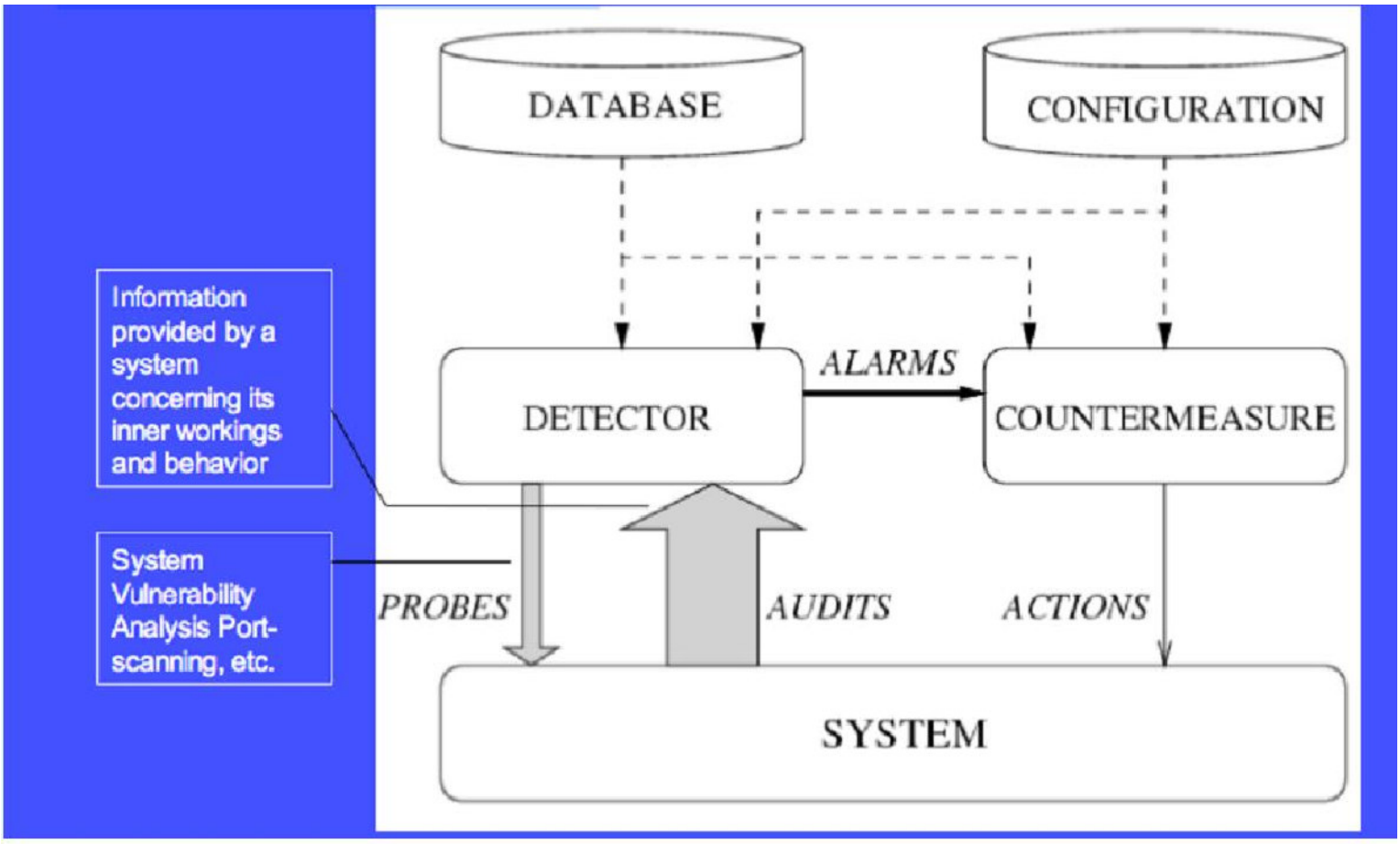
Insertion حمله



ترکیب HIDS و NIDS



Generic IDS


DATABASE
CONFIGURATION
Information provided by a system concerning its inner workings and behavior
ALARMS
DETECTOR
COUNTERMEASURE
System Vulnerability Analysis Port-scanning, etc.
PROBES
AUDITS
ACTIONS
SYSTEM

مثال هایی از IDS

- مبتنی بر امضاء
  - Snort –
  - STAT –
  - Bro –
- مبتنی بر ناهنجاری
  - MADAM ID –
  - ADAM –