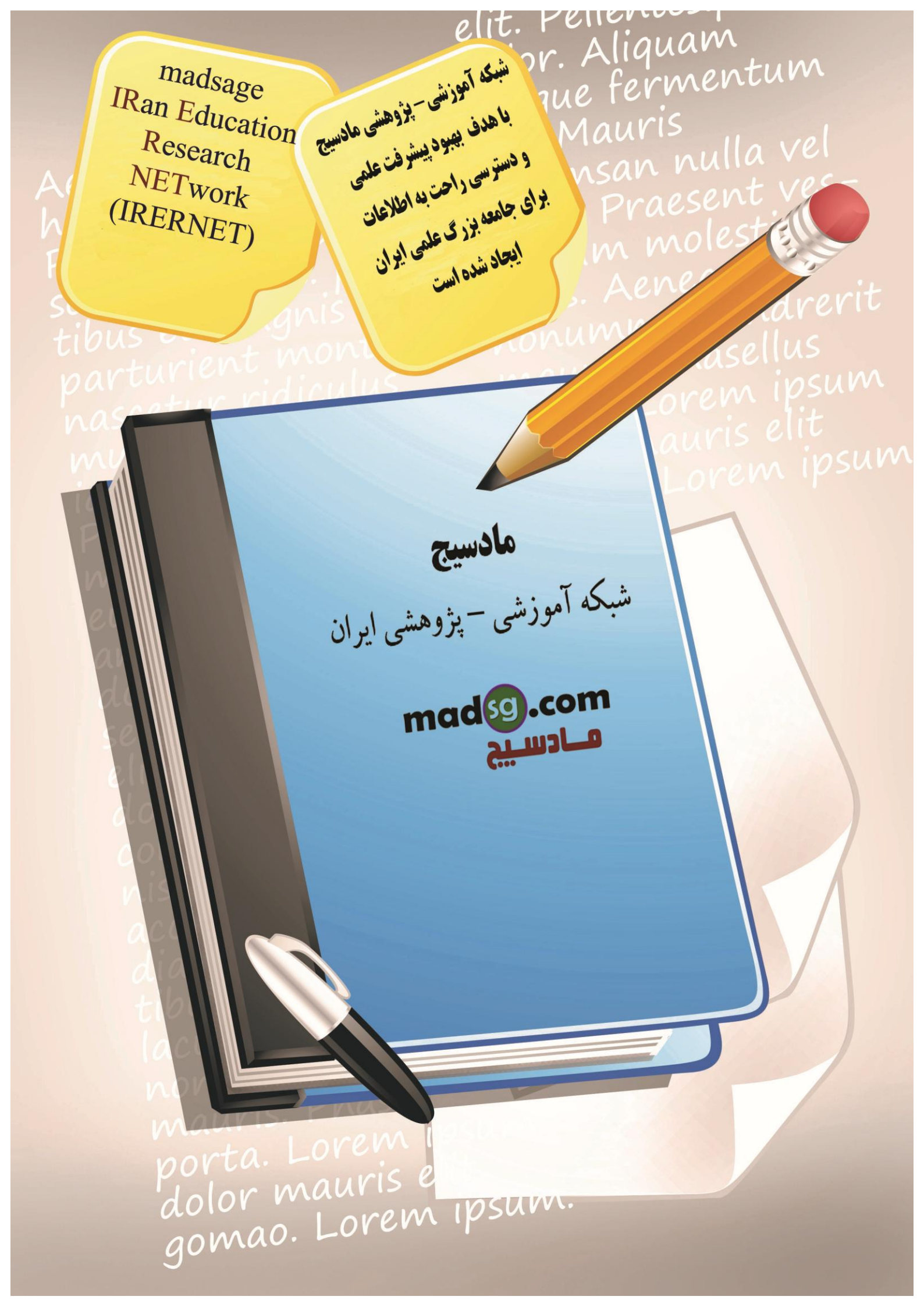

madsage
IRan Education
Research
NETwork
(IRERNET)
شبکه آموزشی-پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است
مادسیج
شبکه آموزشی - پژوهشی ایران
madsg.com
مادسیج

یا ذاالامن والامان

امنیت داده و شبکه

سیستم تشخیص نفوذ

مرتضی امینی - نیمسال اول ۹۱-۹۰

مرکز امنیت داده و شبکه شریف
http://dnsl.ce.sharif.edu

فهرست مطالب

- مقدمه و تعاریف اولیه
- تاریخچه سیستم‌های تشخیص نفوذ
- رده‌بندی و مشخصات سیستم‌های تشخیص نفوذ
- پیاده‌سازی سیستم‌های تشخیص نفوذ
- معرفی چند سیستم تشخیص نفوذ نمونه
- مکمل سیستم‌های تشخیص نفوذ

سیستم تشخیص نفوذ

- **تشخیص نفوذ (ID):** فرآیند نظارت بر وقایع رخ داده در یک شبکه و یا سیستم کامپیوتری در جهت کشف موارد انحراف از سیاست‌های امنیتی.
- **سیستم تشخیص نفوذ (IDS):** یک نرم‌افزار با قابلیت تشخیص، آشکارسازی و پاسخ (واکنش) به فعالیت‌های غیرمجاز یا ناهنجار در رابطه با سیستم.
- تحقیقات و توسعه آن از سال ۱۹۸۰ به بعد

وظایف عمومی یک IDS

- نظارت و تحلیل فعالیت‌های شبکه، سیستم و کاربر
- بررسی پیکربندی سیستم و آسیب‌پذیری‌ها
- ارزیابی صحت سیستم و فایل‌های داده‌ای حساس
- تشخیص الگوهای منطبق با حملات شناخته شده
- تحلیل آماری الگوهای فعالیت ناهنجار
- در بعضی موارد:
  - نصب خودکار وصله‌های نرم‌افزاری ارائه شده
  - نصب و اجرای کارگزاران تله‌عسل برای کسب اطلاعات بیشتر

دلایل استفاده از سیستم‌های تشخیص نفوذ

- جلوگیری از رفتارهای مشکل‌زا با مشاهده خطرات کشف شده
- تشخیص و مقابله با مقدمات حملات
- ثبت تهدیدات موجود برای یک سازمان
- اطلاعات مفیدی درباره تهاجمات و نفوذهایی که واقع می‌شوند، ارائه می‌دهد و امکان عیب‌یابی، کشف، و تصحیح عامل‌های سبب شونده را فراهم می‌کند.

هدف IDS

- **حسابرسی:** قابلیت ارتباط دادن یک واقعه به شخص مسئول آن واقعه

  (نیازمند مکانیزم‌های شناسایی و ردیابی)

- **پاسخگویی (واکنش):** قابلیت شناخت حمله و سپس انجام عملی برای مقابله یا توقف آن (و پیشگیری از تکرار آن)

فهرست مطالب

- مقدمه و تعاریف اولیه
- **تاریخچه سیستم‌های تشخیص نفوذ**
- رده‌بندی و مشخصات سیستم‌های تشخیص نفوذ
- پیاده‌سازی سیستم‌های تشخیص نفوذ
- معرفی چند سیستم تشخیص نفوذ نمونه
- مکمل سیستم‌های تشخیص نفوذ

تاریخچه

- ممیزی: فرایند تولید، ثبت و مرور یک سابقه تاریخی از وقایع سیستم (اواخر دهه ۷۰ و اوایل دهه ۸۰)
  - ترمیم در موقع بروز خطا
  - بازسازی وقایع سیستم
  - کشف سوء استفاده‌ها
- اطلاعات ثبت شده
  - زمان و تاریخ رویداد
  - شناسه کاربر ایجاد کننده آن رویداد (این شناسه باید برای هر کاربر یکتا باشد)
  - نوع رویداد یا حادثه
  - موفقیت یا شکست آن رویداد

تاریخچه – نسل اول

- ۱۹۸۰

- **سیستم‌های مبتنی بر میزبان**
  - جمع‌آوری داده‌ها در سطح سیستم‌عامل جهت تحلیل
  - پیدایش مفهوم ناهنجاری (anomaly) و سوءاستفاده (misuse)

- مثال: سیستم IDES

تاریخچه – نسل اول

- تشخیص ناهنجاری: تولید نمایه برای هر کاربر بر اساس ویژگی‌ها (نرخ تایپ، مدت نشست، تعداد فایل‌های باز شده، فرمان‌های صادر شده و ...)
- تشخیص سوءاستفاده: شناخت نقاط آسیب‌پذیر سیستم

ظهور شبکه‌های کامپیوتری و افزایش قابلیت دسترسی از راه دور

- پیدایش حملات و نفوذهای شبکه‌ای

تاریخچه – نسل دوم

- ۱۹۹۰
- **سیستم‌های مبتنی بر شبکه**
  - جمع‌آوری داده‌ها از ترافیک شبکه

- تشخیص ناهنجاری: استخراج ویژگی‌های ترافیک عادی در شبکه
- تشخیص سوء استفاده: شناخت حملات شبکه و تاثیر آنها بر ترافیک شبکه

رشد و توسعه اینترنت و سیستم‌های باز

- مثال: NSM

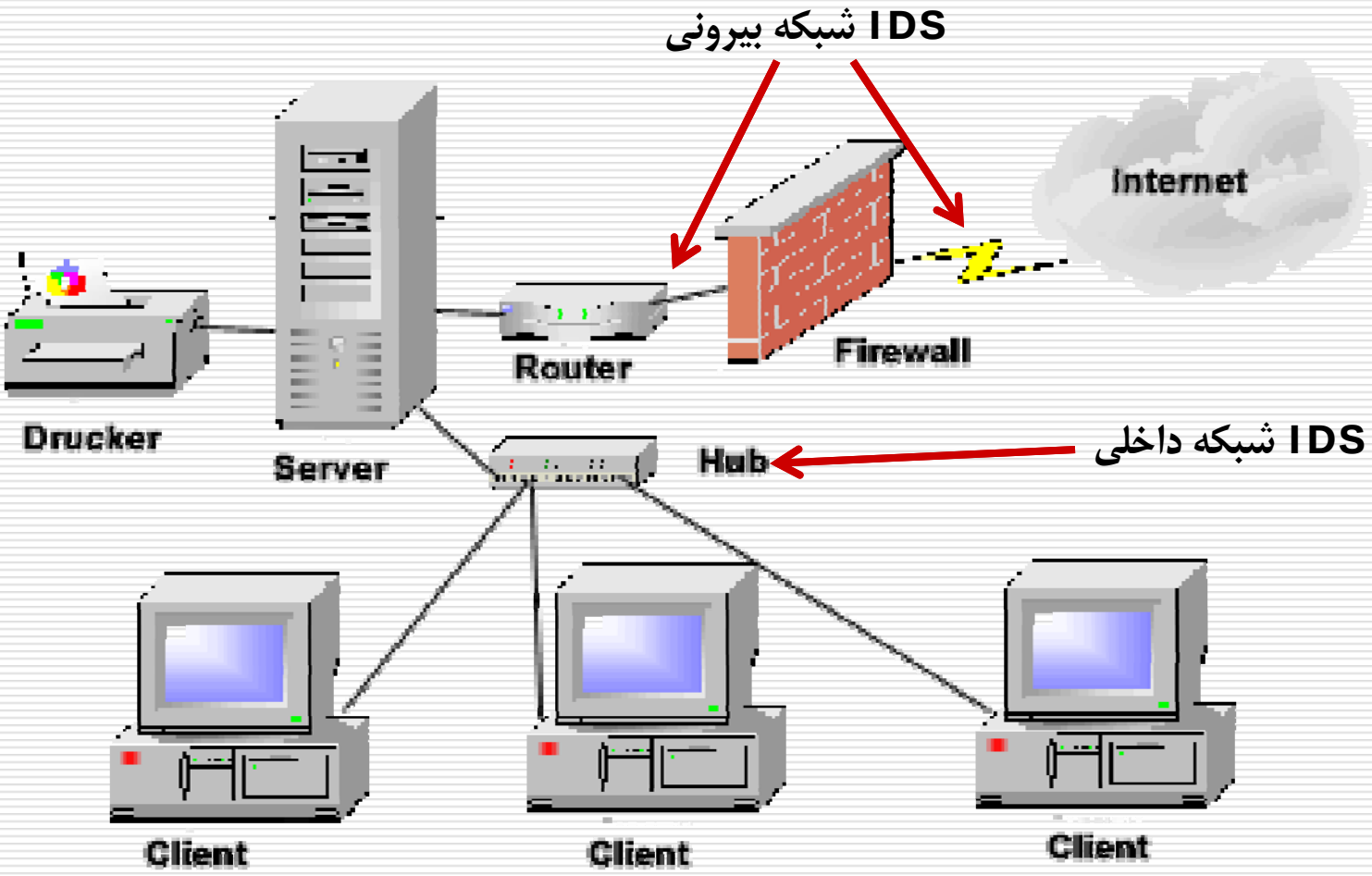
تاریخچه – نسل سوم

- **سیستم‌های تشخیص نفوذ مبتنی بر منابع ناهمگون**
  - جمع آوری داده‌ها هم از میزبان و هم از شبکه
  - معماری توزیع‌شده (در جمع‌آوری و تحلیل)
  - سیستم‌های مبتنی بر عامل (Agent)
- مثال: AAFID، DIDS و EMERALD
- ظهور محصولات تجاری و کاربردی

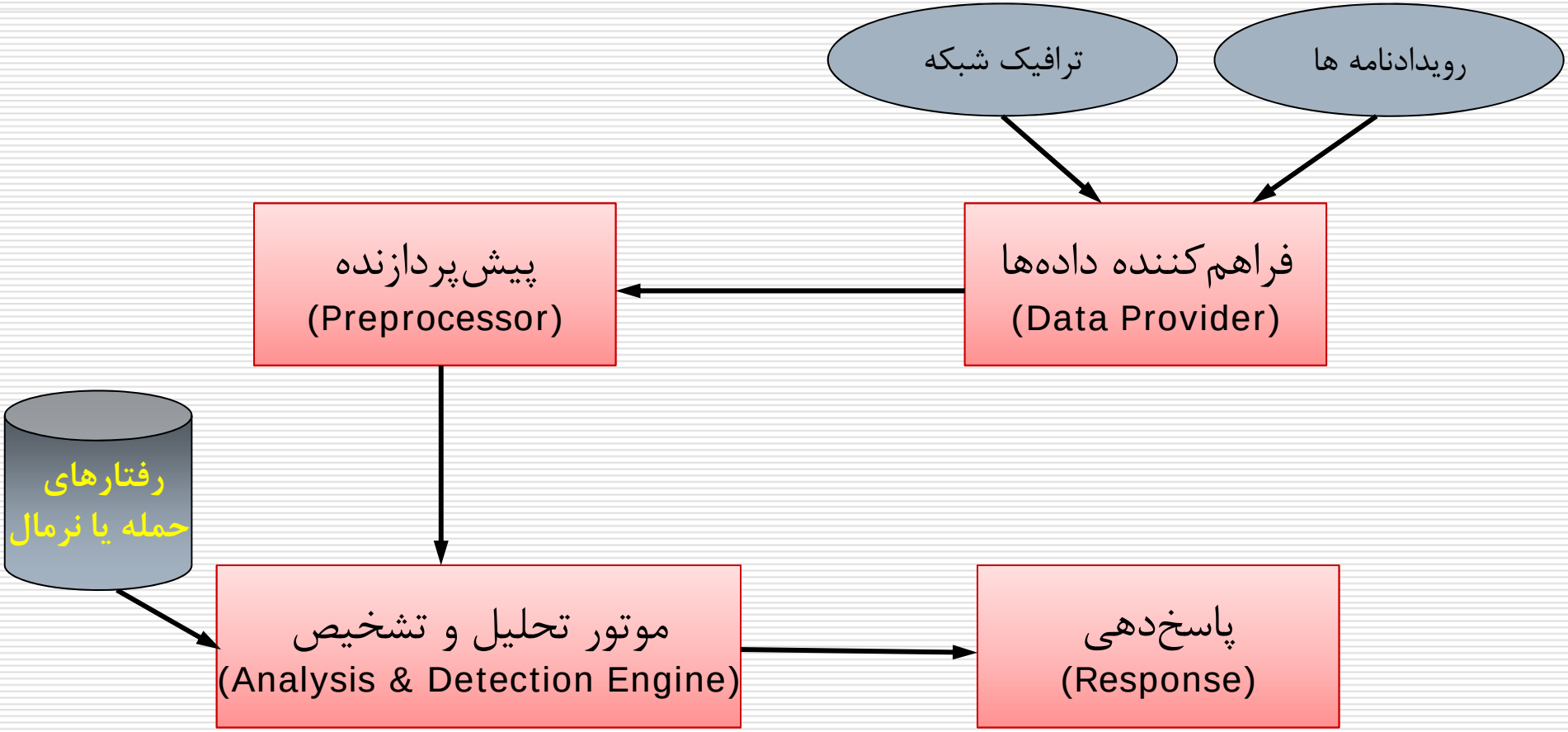
فهرست مطالب

- مقدمه و تعاریف اولیه
- تاریخچه سیستم‌های تشخیص نفوذ
- **رده‌بندی و مشخصات سیستم‌های تشخیص نفوذ**
- پیاده‌سازی سیستم‌های تشخیص نفوذ
- معرفی چند سیستم تشخیص نفوذ نمونه
- مکمل سیستم‌های تشخیص نفوذ

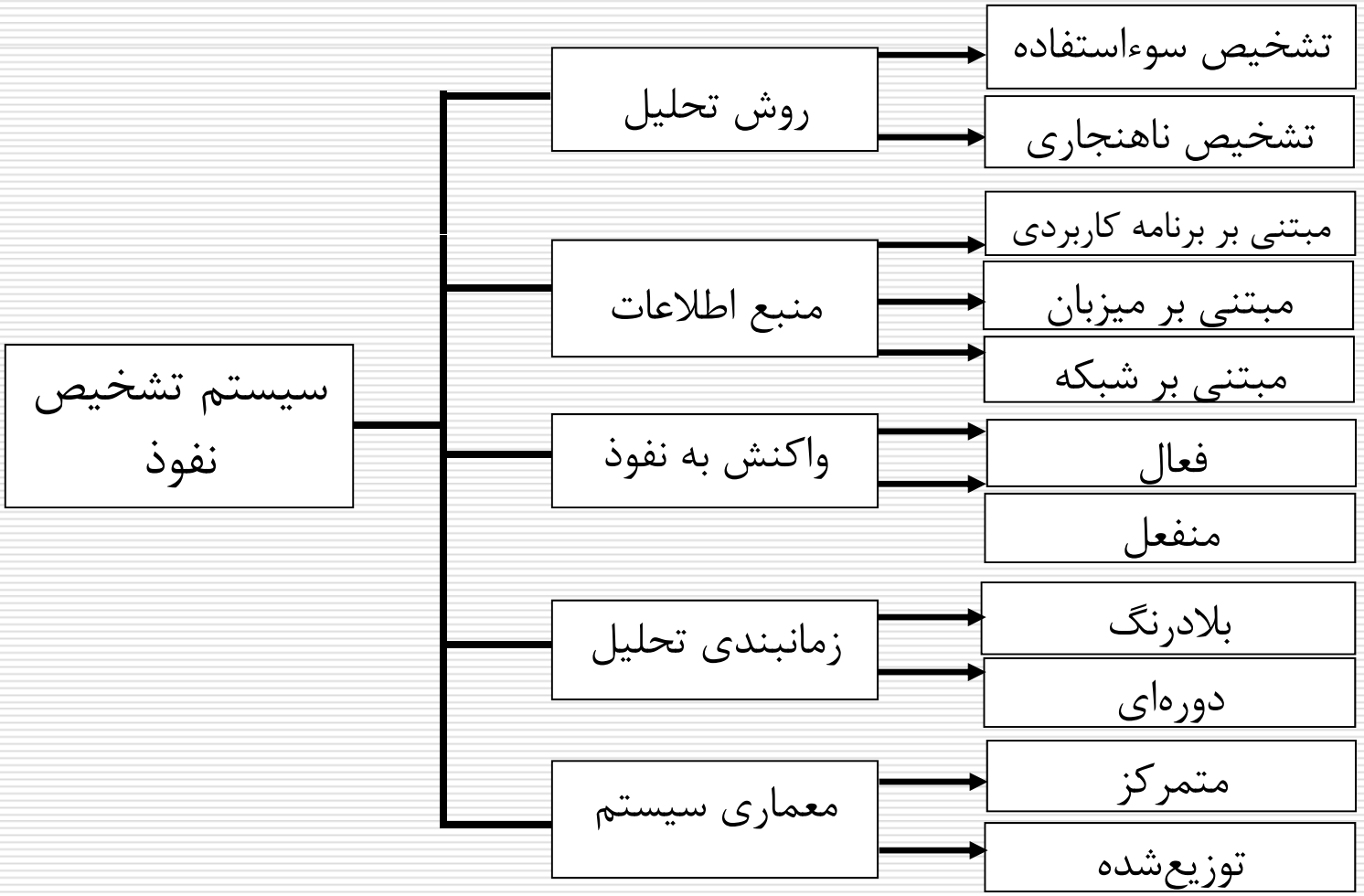
آرایش قرارگیری IDS در شبکه



معماری یک IDS

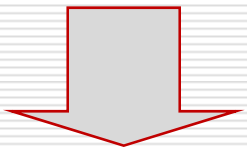


رده‌بندی کلی سیستم‌های تشخیص نفوذ



جمع آوری اطلاعات

- عملیات جمع‌آوری داده از یک منبع اطلاعاتی و تحویل آنها به پیش‌پردازنده و موتور تحلیل



- **مبتنی بر شبکه** ترافیک شبکه
- **مبتنی بر میزبان** دنباله‌های ممیزی سیستم‌عامل، رویدادنامه‌ها
- **مبتنی بر برنامه کاربردی** رویدادنامه پایگاه‌داده‌ها، رویدادنامه کارگزار وب

جمع آوری اطلاعات (ادامه)

تشخیص نفوذ مبتنی بر شبکه

مزایا:

- قابلیت نظارت بر یک شبکه بزرگ
- عدم تداخل با عملکرد معمولی شبکه
- قابلیت مخفی نگه‌داشته شدن از دید مهاجمان

معایب:

- عدم عملکرد صحیح در ترافیک سنگین
- عدم توانایی در تحلیل اطلاعات رمز شده (مانند VPN)

جمع آوری اطلاعات (ادامه)

نظارت مبتنی بر میزبان

مزایا:

- کشف حملاتی که از طریق شبکه قابل شناسایی نیستند.
- قابلیت عمل در محیطی که ترافیک شبکه در آن رمز شده

معایب:

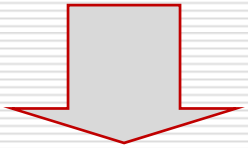
- امکان غیرفعال شدن سیستم در بخشی از حمله
- نیاز به انباره زیاد برای ذخیره اطلاعات
- سربار محاسباتی برای میزبان

زمانبندی تحلیل

- زمانبندی(Timing): فاصله زمانی بین رخداد وقایع در منبع اطلاعات تا تحلیل آنها توسط موتور تحلیل
- زمانبندی دسته‌ای یا دوره ای (Batch)
  - کشف نفوذ پس از وقوع، عدم امکان پاسخ‌گویی فعال
- زمان‌بندی بلادرنگ (Real-time)
  - تشخیص نفوذ به محض وقوع و یا حتی قبل از آن، وجود امکان پاسخ‌گویی فعال و پیش‌گیری از نفوذ

تحلیل و تشخیص

- سازمان‌دهی اطلاعات و جستجوی علائم امنیتی



علائم حمله

- **تشخیص سوء استفاده**
- **تشخیص ناهنجاری**

رفتار غیرنرمال

تحلیل و تشخیص
(تشخیص سوء استفاده)

- مشخصات
  - شناخت حملات موجود
  - تعریف الگوی حملات برای موتور تحلیل
  - جستجوی مجموعه‌ای از وقایع که با یک الگوی از پیش تعریف شده مطابقت دارد.
  - نیاز به بروزرسانی الگوهای حمله
- روشهای پیاده‌سازی: سیستم خبره، روشهای مبتنی بر گذار حالات و ...
- کاربرد در سیستم‌های تجاری IDS

تحلیل و تشخیص
(تشخیص ناهنجاری)

- مشخصات
  - شناخت عملکرد نرمال سیستم
  - تهیه نمایه‌هایی از رفتار نرمال سیستم برای موتور تحلیل
  - جستجوی فعالیت غیرنرمال

آیا هر رفتار غیر نرمال یک حمله است ؟

- روشهای پیاده‌سازی: روشهای آماری، شبکه‌های عصبی و ...
- بیشتر جنبه‌های تحقیقاتی تا کاربردی

تحلیل و تشخیص (مقایسه)

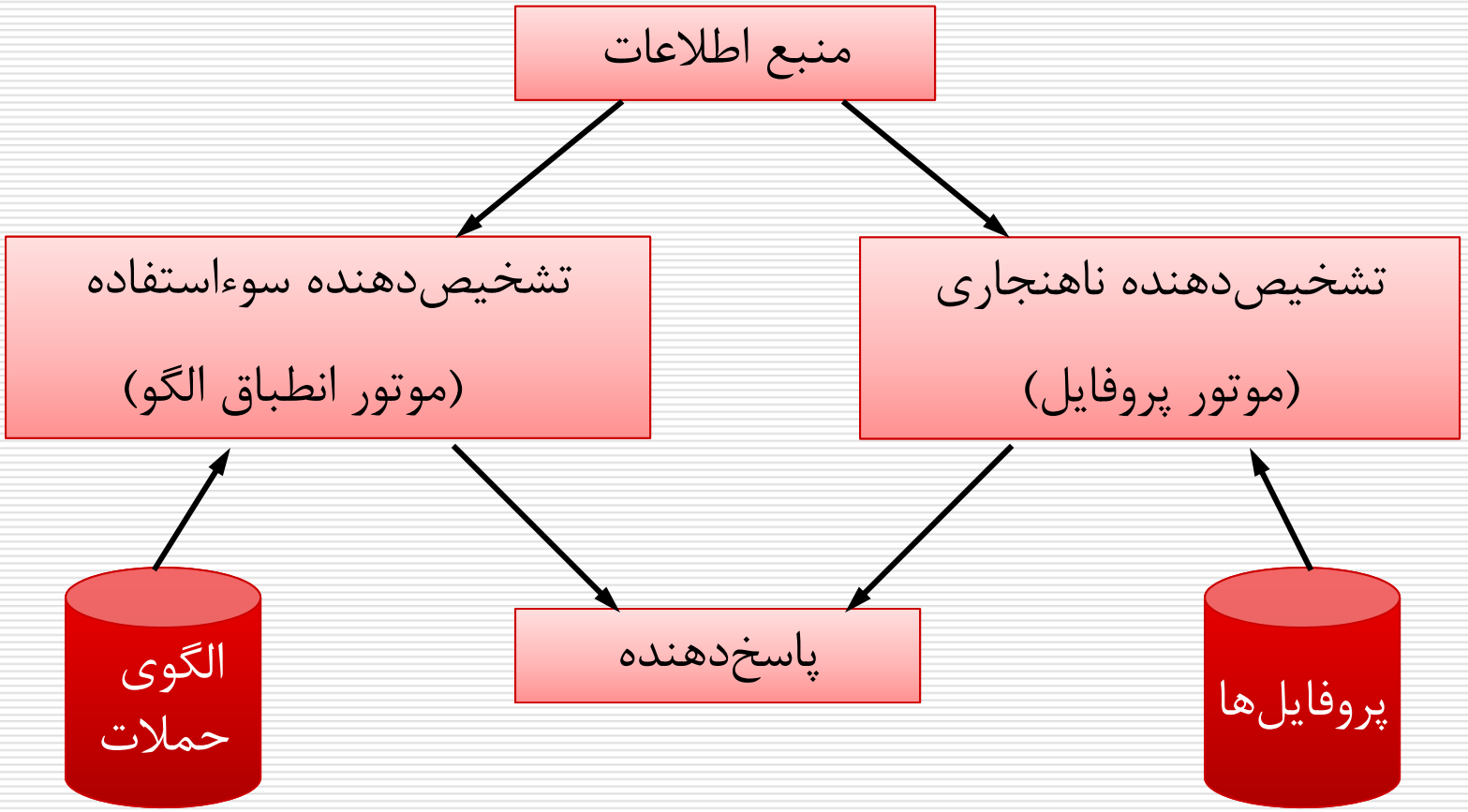
تشخیص سوءاستفاده Misuse Detection	تشخیص ناهنجاری Anomaly Detection
تشخیص فقط در حد حملات شناخته شده	تشخیص حملات ناشناخته
تشخیص سریع و مطمئن با خطای کمتر	بالابودن درصد خطای مثبت غلط

مثبت غلط: تشخیص نادرست نرمال به حمله (حمله تشخیص داده شده ولی نرمال است)

منفی غلط: تشخیص نادرست حمله به نرمال (نرمال تشخیص داده شده ولی حمله است)

تحلیل و تشخیص (ترکیب)

نمای یک سیستم تشخیص نفوذ ترکیبی



واکنش به نفوذ

- فعال (Active): انجام برخی اعمال واکنشی به صورت خودکار
  - انجام عملی علیه مهاجم
  - جمع‌آوری اطلاعات بیشتر

سیستم جلوگیری از نفوذ (IPS)

- منفعل (Passive): گزارش به مدیران و واگذاری واکنش به آنها
  - نمایش پیغام بر روی صفحه
  - ارسال پست الکترونیکی

فهرست مطالب

- مقدمه و تعاریف اولیه
- تاریخچه سیستم‌های تشخیص نفوذ
- رده‌بندی و مشخصات سیستم‌های تشخیص نفوذ
- **پیاده‌سازی سیستم‌های تشخیص نفوذ**
- معرفی چند سیستم تشخیص نفوذ نمونه
- مکمل سیستم‌های تشخیص نفوذ

روشهای پیاده‌سازی تشخیص سوءاستفاده

- **سیستم خبره**

مکانیزمی برای پردازش حقایق و مشتق کردن نتایج منطقی از این حقایق با توجه به زنجیره‌ای از قواعد

قواعد ⟵ الگوها یا سناریوهای نفوذ

حقایق ⟵ وقایع رخ‌داده در سیستم

روش‌های پیاده‌سازی تشخیص سوءاستفاده

مزایا

- ارائه حملات در قالب قواعد توسط کاربر بدون نیاز به دانستن نحوه عملکرد سیستم خبره
- امکان اضافه کردن قواعد جدید بدون تغییر قواعد قبلی

معایب

- کارآیی پایین، نامناسب برای حجم زیاد داده‌ها
- نامناسب برای بیان ترتیب در قواعد

روش‌های پیاده‌سازی تشخیص سوءاستفاده

روش‌های مبتنی بر گذار حالت

- استفاده از مفهوم حالت سیستم وگذار
- استفاده از تکنیک‌های انطباق الگو
- سرعت و قابلیت

الگوی حمله : **حالت امن اولیه** ←(عملیات کلیدی)— **حالت خطرناک نهایی**

روش‌های پیاده‌سازی تشخیص ناهنجاری

- **روش‌های مبتنی بر کاربر**
  - تولید نمایه از رفتار نرمال کاربران
  - مقایسه رفتار واقعی کاربران با نمایه‌ها و یافتن رفتارهای غیرنرمال
- **روش‌های مبتنی بر پردازه**
  - بیان رفتار نرمال پردازه‌ها با رشته‌ای از فراخوانی‌های سیستمی
  - نظارت بر رفتار واقعی پردازه و یافتن رفتارهای غیرنرمال

روش‌های پیاده‌سازی تشخیص ناهنجاری مبتنی بر کاربر

- تحلیل کمی: بیان نمایه با معیارهای عددی
  - تعداد مجاز ورود ناموفق برای کاربر A، n است.
- تحلیل آماری: بیان نمایه با معیارهای آماری
  - ورودهای ناموفق برای کاربر A تابع توزیع نرمال a است.
  - IDES، NIDES، Haystack

روش‌های پیاده‌سازی تشخیص ناهنجاری مبتنی بر کاربر

- روش‌های مبتنی بر قاعده: بیان معیارهای آماری با مجموعه‌ای از قواعد
  - استفاده از سیستم خبره برای بیان نمایه‌ها
- شبکه‌های عصبی: استخراج نمایه از سابقه سیستم
- الگوریتم ژنتیک: تعریف بردار فرضی (نفوذ یا عدم‌نفوذ) برای واقعه، آزمون اعتبار فرض، اصلاح و بهبود فرض

روش‌های پیاده‌سازی تشخیص ناهنجاری مبتنی بر پردازه

- روش سیستم ایمنی
  - بیان رفتار نرمال پردازه با ترتیب زمانی بین فراخوانی‌ها نه فراوانی یا توزیع و یا اهمیت آنها
- داده‌کاوی
  - کشف الگوهای مفید در رفتار نرمال پردازه و استفاده از آنها برای تعیین رفتار غیرنرمال

روش‌های پیاده‌سازی تشخیص ناهنجاری مبتنی بر پردازه

- مدل مارکوف: بیان رفتار نرمال پردازه توسط ماشین‌های با حالات متناهی

- روش مبتنی بر توصیف: بیان رفتار نرمال پردازه با استفاده از یک زبان توصیف
  - مثال: زبان ASL ، گرامر شبه منظم

پیاده سازی سیستمهای تشخیص نفوذ توزیع شده

- سیستم‌های تشخیص نفوذ مبتنی بر عامل
  - عامل: یک موجود نرم‌افزاری برای انجام یک عمل نظارتی (جمع‌آوری داده) یا امنیتی (تحلیل) خاص در یک میزبان
- تشخیص مبتنی بر عامل
  - جمع‌آوری داده توزیع شده
  - تحلیل توزیع شده
  - EMERALD و AAFID

فهرست مطالب

- مقدمه و تعاریف اولیه
- تاریخچه سیستم‌های تشخیص نفوذ
- رده‌بندی و مشخصات سیستم‌های تشخیص نفوذ
- پیاده‌سازی سیستم‌های تشخیص نفوذ
- **معرفی چند سیستم تشخیص نفوذ نمونه**
- مکمل سیستم‌های تشخیص نفوذ

معرفی چند سیستم تشخیص نفوذ نمونه

- سیستم Snort
  - یک IDS رایگان
  - مبتنی بر شبکه
  - تشخیص سوءاستفاده مبتنی بر توصیف حملات
  - حاوی الگوی هزاران نوع حمله
  - با قابلیت Sniffing و Packet logging

معرفی چند سیستم تشخیص نفوذ نمونه

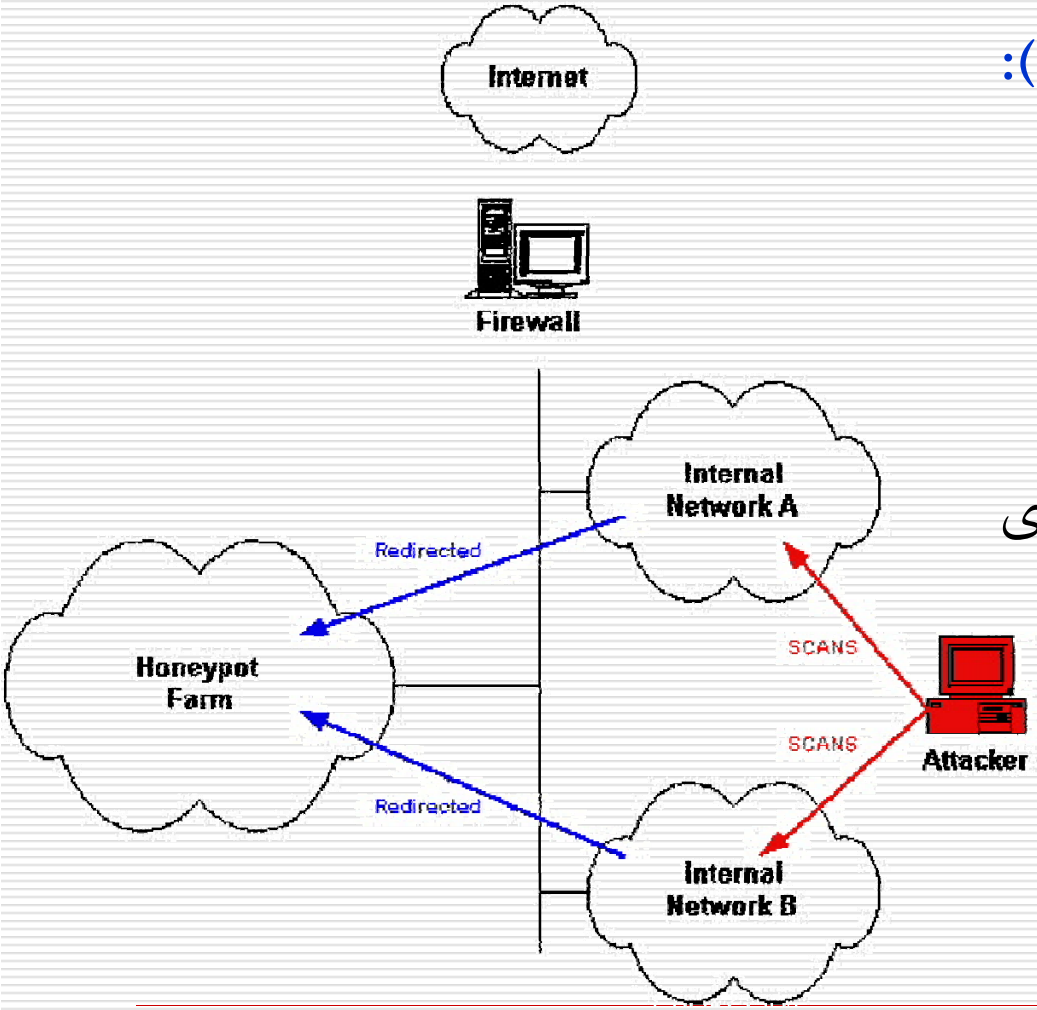
سیستم OSSEC

- سیستم تشخیص نفوذ مبتنی بر میزبان
- امکان تحلیل رویدادنامه، کنترل صحت، مانیتورینگ رجیستری ویندوز
- پاسخ‌دهی دوره‌ای و پاسخ‌دهی فعال
- قابلیت به کارگیری در سیستم‌های عامل‌های مختلف (مانند Linux، FreeBSD، Mac OS، و Windows)

فهرست مطالب

- مقدمه و تعاریف اولیه
- تاریخچه سیستم‌های تشخیص نفوذ
- رده‌بندی و مشخصات سیستم‌های تشخیص نفوذ
- پیاده سازی سیستم‌های تشخیص نفوذ
- معرفی چند سیستم تشخیص نفوذ نمونه
- **مکمل سیستم‌های تشخیص نفوذ**

ترکیب با سیستم‌های تله



- **سیستم تله‌عسل (Honeypot):**
  اغفال و فریب مهاجم جهت جمع‌آوری اطلاعات بیشتر از نحوهٔ عملکرد آن.

- درحال حاضر بیشتر برای جمع‌آوری بدافزارها استفاده می‌شود.

- استفاده از سیستم‌های تشخیص ناهنجاری برای هدایت ترافیک مشکوک به تله‌ها

تحلیل همبستگی رویدادها

Log Correlation Systems

- سیستمی برای تحلیل همبستگی بین رویدادهای ثبت شده توسط سیستم‌های تشخیص نفوذ

اهداف:

- کاهش حجم اعلان‌ها
- استخراج حملات چندمرحله‌ای

پایان

مرکز امنیت داده و شبکه شریف

http://dnsl.ce.sharif.edu

پست الکترونیکی

m_amini@ce.sharif.edu

شبکه آموزشی- پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است

madsg.com

مادسیج

IRan Education & Research NETwork
(IRERNET)