یا ذاالامن والامان

سیســـتم تشخـــیص نفـــوذ

مبانی امنیت اطلاعات و شبکه‌های کامپیوتری

محمدرضا رازیان*

بهار و تابستان 1395

مرکز تخصصی آپا

دانشگاه سمنان

مرکز تخصصی آپا دانشگاه سمنان

http://cert.semnan.ac.ir

آزمایشگاه امنیت داده و شبکه شریف

http://dnsl.ce.sharif.ir

*Homepage: www.mrazian.com

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
- مبهم سازی

سیستم تشخیص نفوذ

- **تشخیص نفوذ (Intrusion Detection)**: فرآیند نظارت بر وقایع رخ داده در یک شبکه و یا سیستم کامپیوتری در جهت کشف موارد انحراف از سیاست‌های امنیتی.
- **سیستم تشخیص نفوذ (Intrusion Detection System)**: 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 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

- تشخیص و ثبت تهدیدات موجود برای یک سازمان
- جلوگیری از کامل شدن حملات با تشخیص در مراحل اولیه
- جلوگیری از تکرار حملات مشابه با آگاهی رسانی در مورد حملات کشف شده
- جمع‌آوری اطلاعات مفید درباره حملات و نفوذهای اتفاق افتاده و فراهم‌سازی امکان عیب‌یابی (شناخت آسیب‌پذیری‌ها)، کشف، و تصحیح عامل‌های سبب شونده

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

تاریخچه

- **ممیزی (Audit):** 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

در IDSبه دنبال خودکارسازی ممیزی بوده‌اند.

تاریخچه – نسل اول

- ۱۹۸۰

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

- مثال: سیستم IDES
  - (Intrusion Detection Expert System)

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
  - Network Security Monitorin

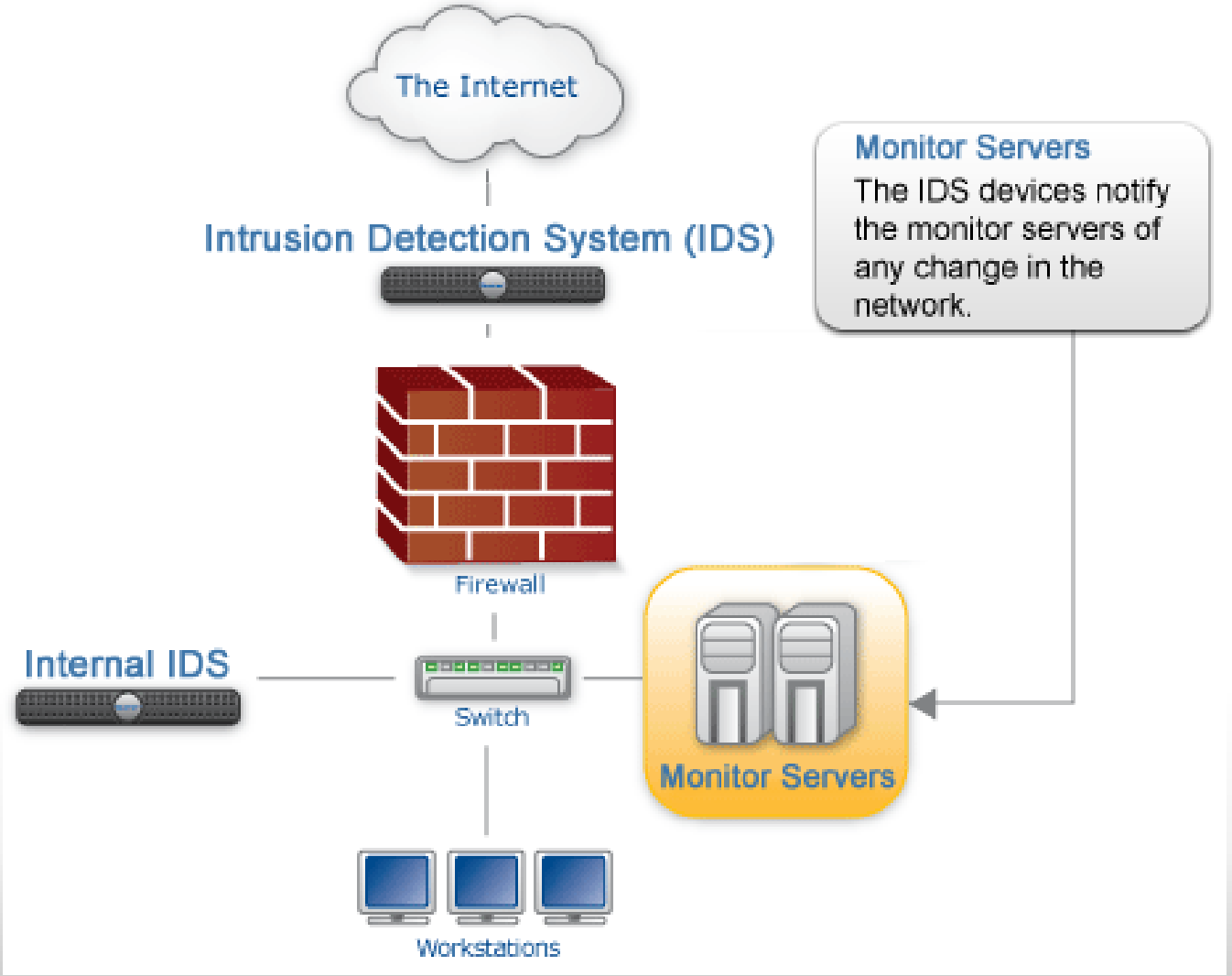
تاریخچه – نسل سوم

- **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)

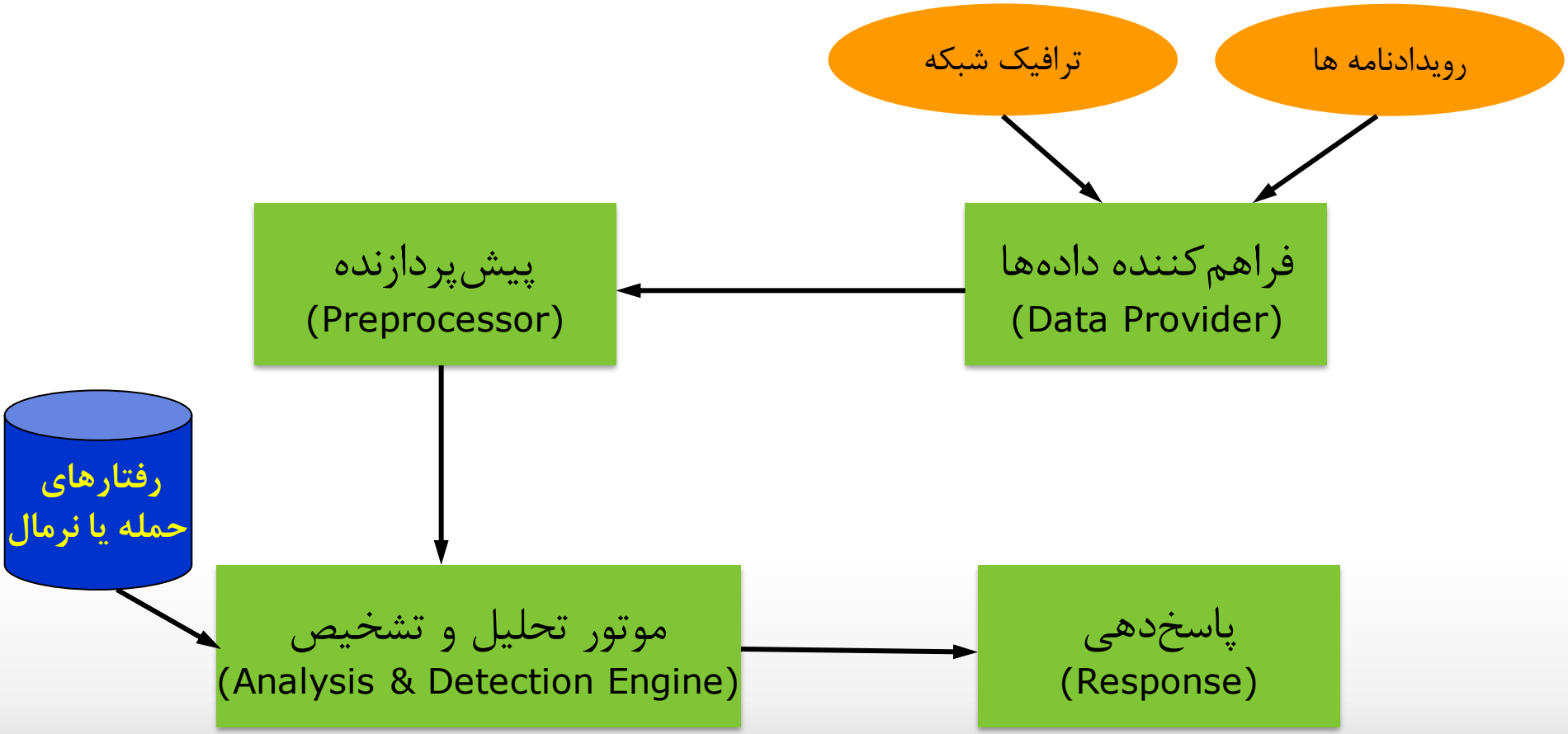
- مثال:
  - AAFID (Autonomous Agent for Intrusion Detection)
  - DIDS (Distributed IDS)
  - EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances)

فهرست مطالب

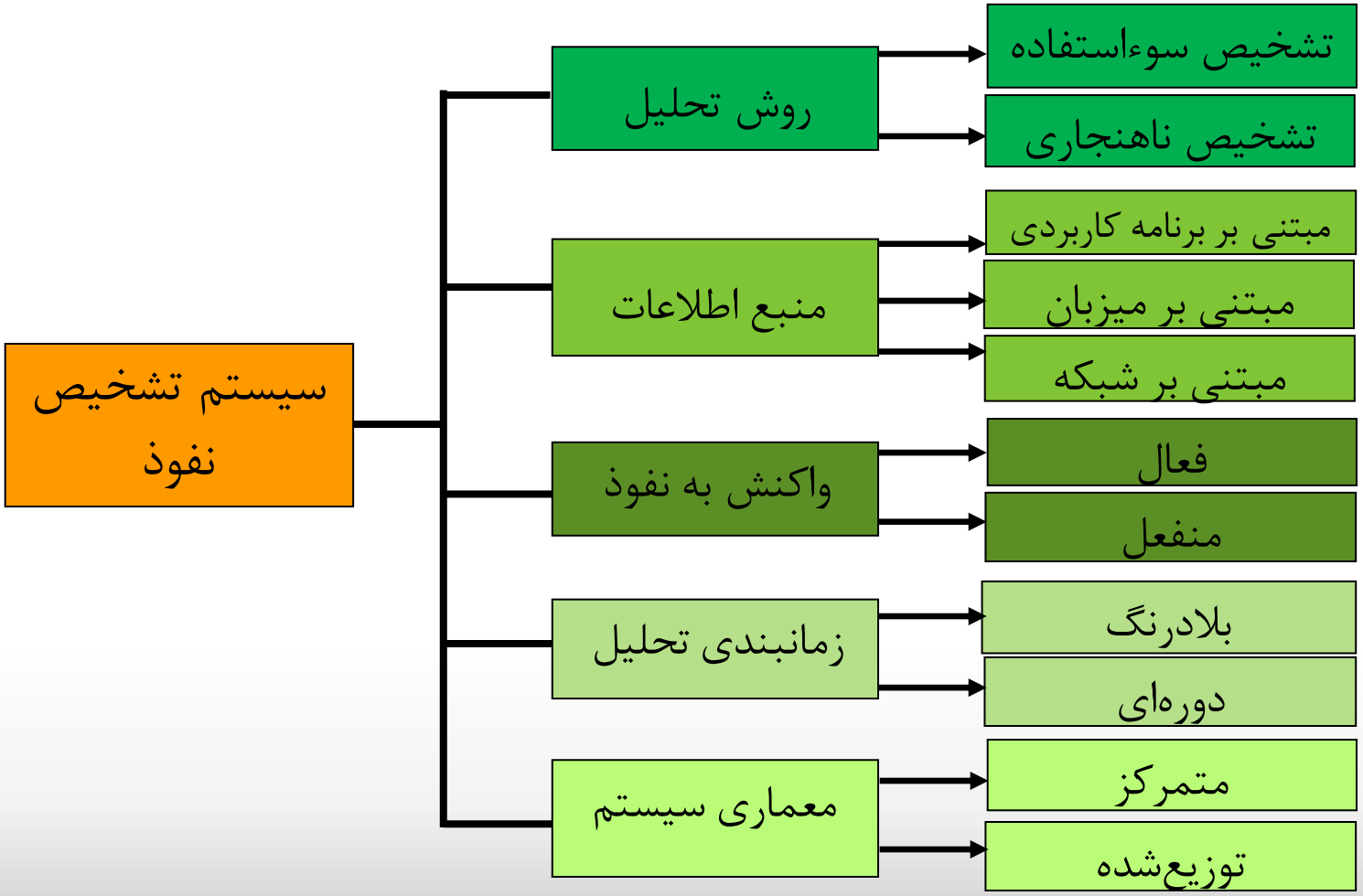
آرایش قرارگیری IDS در شبکه



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 (Audit Trail)، رویدادنامه‌ها (Logs)
- **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:

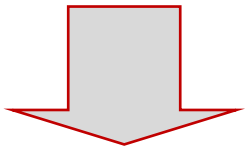
- امکان غیرفعال شدن سیستم در بخشی از حمله
- نیاز به انباره زیاد برای ذخیره اطلاعات
- سربار محاسباتی برای میزبان

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 ...

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

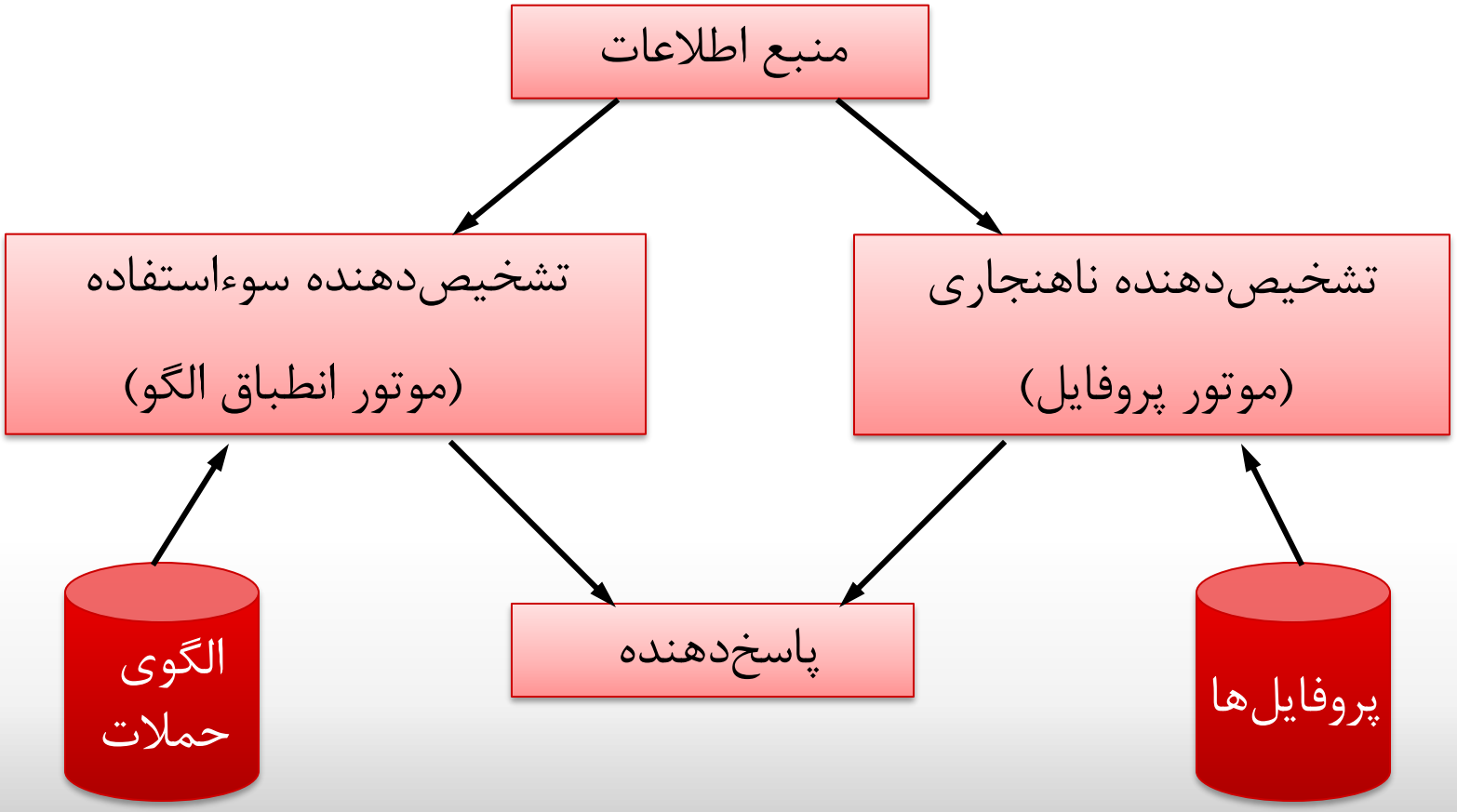
مثبت غلط: تشخیص نادرست نرمال به حمله (حمله تشخیص داده شده ولی نرمال است)

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

	Disease or Condition	No Disease or Condition
Test Positive	A True Positive	B False Positive
Test Negative	C False Negative	D True Negative

تحلیل و تشخیص (ترکیب)

- نمای یک سیستم تشخیص نفوذ ترکیبی



واکنش به نفوذ

- فعال (Active): در صورت تشخیص حمله انجام برخی اعمال واکنشی به صورت خودکار
  - انجام عملی علیه مهاجم (مثلا انسداد دسترسی مها جم)
  - جمع‌آوری اطلاعات بیشتر

عنوان دیگر IDSهای فعال:

سیستمهای جلوگیری از نفوذ (IPS)

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

فهرست مطالب

روشهای پیاده‌سازی تشخیص سوءاستفاده

- **سیستم خبره**

مکانیزمی برای پردازش حقایق و استنتاج 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

معرفی چند سیستم تشخیص نفوذ نمونه

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


```
root@mohammad-Studio-1558:/etc/snort/rules# ls
attack-responses.rules          community-nntp.rules          deleted.rules       netbios.rules    sql.rule
backdoor.rules                  community-oracle.rules        dns.rules           nntp.rules       telnet.r
bad-traffic.rules               community-policy.rules        dos.rules           oracle.rules     tftp.rul
chat.rules                      community-sip.rules           experimental.rules  other-ids.rules  virus.ru
community-bot.rules             community-smtp.rules          exploit.rules       p2p.rules        web-atta
community-deleted.rules         community-sql-injection.rules finger.rules        policy.rules     web-cgi.
community-dos.rules             community-virus.rules         ftp.rules           pop2.rules       web-clie
community-exploit.rules         community-web-attacks.rules   icmp-info.rules     pop3.rules       web-colo
community-ftp.rules             community-web-cgi.rules       icmp.rules          porn.rules       web-fron
community-game.rules            community-web-client.rules    imap.rules          rpc.rules        web-iis.
community-icmp.rules            community-web-dos.rules       info.rules          rservices.rules  web-misc
community-imap.rules            community-web-iis.rules       local.rules         scan.rules       web-php.
community-inappropriate.rules   community-web-misc.rules      misc.rules          shellcode.rules  x11.rule
community-mail-client.rules     community-web-php.rules       multimedia.rules    smtp.rules
community-misc.rules            ddos.rules                    mysql.rules         snmp.rules
```

root@mohammad-Studio-1558: /home/mohammad

```
# Other ICMP rules are included in icmp-info.rules

alert icmp any any -> any any (msg:"Razian Rule: ICMP Packet"; sid:477; rev:3;)


alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP ISS Pinger"; itype:8; c
ontent:"ISSPNGRQ"; depth:32; reference:arachnids,158; classtype:attempted-recon;
 sid:465; rev:3;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP L3retriever Ping"; icod
e:0; itype:8; content:"ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI"; depth:32; reference:ar
achnids,311; classtype:attempted-recon; sid:466; rev:4;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Nemesis v1.1 Echo"; dsi
```

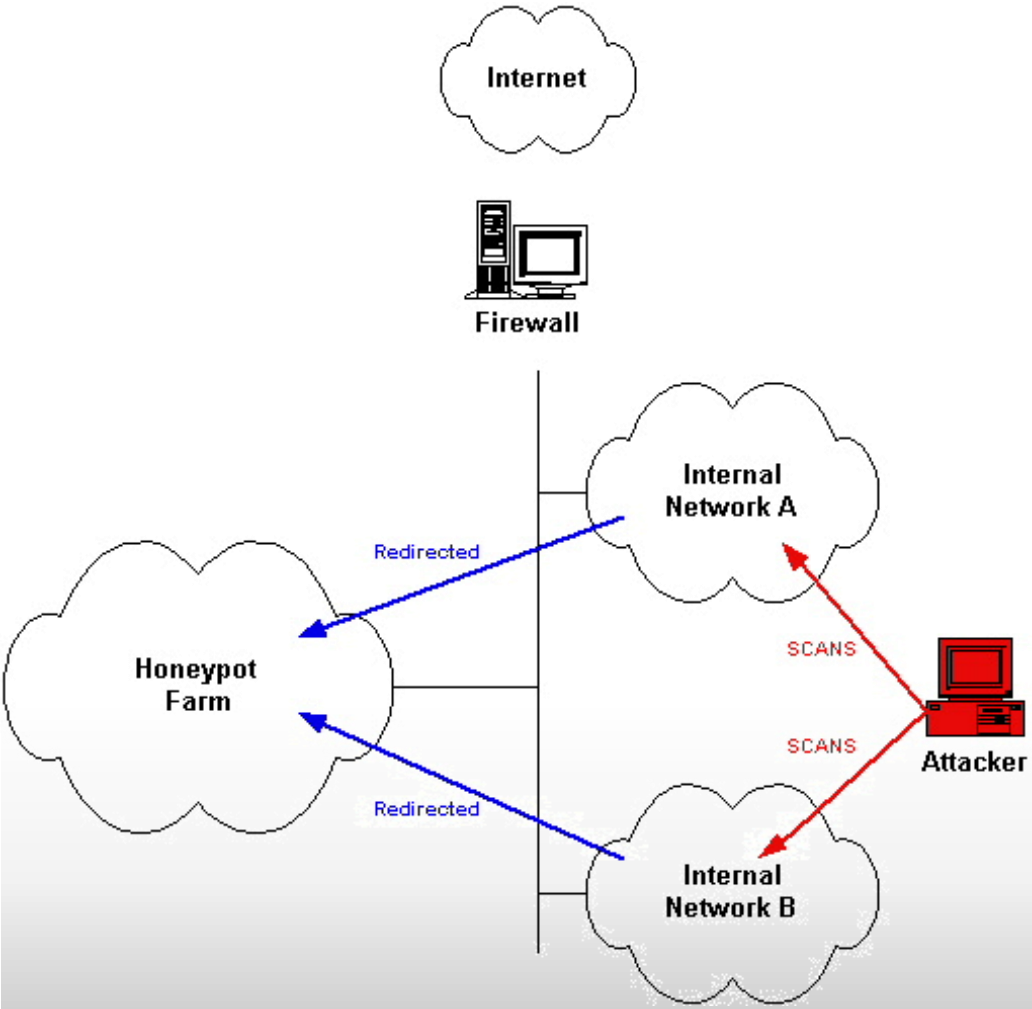
معرفی چند سیستم تشخیص نفوذ نمونه

- **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)

معرفی چند سیستم تشخیص نفوذ نمونه

فهرست مطالب

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.

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

تحلیل همبستگی هشدارها

- سیستم همبسته‌ساز هشدارها Alert Correlation System
- سیستمی برای تحلیل همبستگی بین رویدادهای ثبت شده (هشدارهای تولیده شده توسط سیستم‌های تشخیص نفوذ
- اهداف:
  - کاهش حجم هشدارها و اعلان‌ها
  - وارسی صحت هشدارها
  - استخراج حملات چندمرحله‌ای

فهرست مطالب

مبهم سازی (Obfuscation)

- ایجاد ابهام بدین معناست که هر کسی نتواند معنای اطلاعات مورد نظرمان را بفهمد.
  - شرکت‌های تولید نرم افزار از این ویژگی برای جلوگیری از به‌کارگیری مهندسی معکوس بر روی نرم افزارهایشان، استفاده می‌کنند.
  - هکرها (Hacker)، کرکرها (Cracker) و کلاه سیاه‌ها(Black hot) هم از این روش برای پنهان کردن اطلاعات بدافزار خود (به طوری که مثلاً نتوان اهداف، قصد و نیت بدافزار را با مهندسی معکوس یاد گرفت) استفاده می‌کنند.
- به عنوان مثالی از ایجاد ابهام، مثلاً یک الگو به صورت 5B 50 51 داریم حال بین 51-50 یک کد مثل 90 را وارد می‌کنیم حال الگوی جدید این گونه می‌شود 5B 50 90 51 که دیگر مثل الگوی قبلی نیست و این موضوع باعث می‌شود تا نتوان این الگو را شناسایی کرد. چهار روش ایجاد ابهام عبارتند از:

مبهم سازی (Obfuscation)

- Dead Code Insertion: که یک دستوری که تغییری از نظر منطقی در برنامه ایجاد نمی‌کند را وارد کد می‌کنیم (مثلاً دستور nopsبه معنی انجام هیچ عمل و یا دستورهای Pop, Push متوالی)
- Code transportation: استفاده از دستوراتی مثل انشعاب (Branch) و یا پرش (Jump)
- Register Renaming: تغیراتی در ثبات‌های دستورالعمل‌ها.
- Instruction Substitution: استفاده از کدهایی که از نظر معنایی (Semantic) مشابه هستند اما دارای ساختار (Syntax) متفاوتی هستند. برای شناسایی بد افزارهایی که تکنیک‌های یاد شده در آن‌ها به کار رفته است نیاز به جمع آوری نمونه های مختلف یک نمونه بدافزار را داریم و باید به تحلیل تشابه (Similarity analysis) و یا تولید کدهای نرمال شده بپردازیم.

مبهم سازی (Obfuscation)

- **Similarity Analysis**: در این تحلیل مراحلی برای شناسایی ماهیت برنامه انجام می‌شود. این مراحل به منظور یافتن شباهت‌ها بین دو برنامه است میزان تشابه با یک مقدار آستانه ای مقایسه می‌گردد. و اگر این مقدار خیلی کمتر از مقدار آستانه بود برنامه‌ی در حال بررسی بی خطر و اگرنه یک بدافزار است.
- **Malware Normalization**: در این روش، نرمال‌ساز، نسخه‌ی مبهم شده‌ی یک بدافزار را دریافت می‌کند و تغییرات انجام شده بر روی آن را از بین می‌برد و یک کد نرمال شده تولید می‌کند. بدافزار مورد نظر وارد نرمال ساز می‌شود بعد از نرمال سازی الگوی این بدافزار استخراج می‌گردد و با الگوی های متعارف تطابق داده می‌شود. همچنین این الگوی بدست آمده بعد از نرمال سازی نیز در کنار الگوهای دیگر قرار می‌گیرد تا در مراحل بعد مورد استفاده قرار گیرد.

منابع

- اسلایدهای دکتر مرتضی امینی (منبع اصلی) – درس امنیت داده و شبکه
- Vinod, P., et al. "Survey on malware detection methods." Proceedings of the 3rd Hackers' Workshop on Computer and Internet Security (IITKHACK'09). 2009.
- Idika, Nwokedi, and Aditya P. Mathur. "A survey of malware detection techniques." Purdue University 48 (2007).