

# Advanced Network Security IDS



**Dr. Yaeghoobi**

PhD. Computer Science & Engineering, Networking, India  
[dr.yaeghoobi@gmail.com](mailto:dr.yaeghoobi@gmail.com)

00 | **Current Trends in Cyber Security and Attacks**

01 | **Intrusion Detection System (IDS)**

02 | **Attack Detection**

03 | **Issues of IDS**

04 | **Intrusion Prevention System (IPS)**

# Current Trends in Cyber Security and Attacks

00



# Key Cyber Attacks

- Sony Playstation Network
  - Account information, passwords and credit card numbers breached for 70M users
  - Direct cost of \$170M (Sony)
  - Indirect cost estimated at 10 to 100x
- The IMF (International Monetary Fund)
  - Hack resulted in the loss of a “large quantity” of data, documents and email
- Citigroup
  - More than 200,000 customer accounts hacked
  - Poor web application design made it easy
- Android Apps
  - More than 50% of the third-party apps on Google's official Android Market contained a Trojan called DroidDream, designed to steal personal data

# Fear of the Hack

- 60% of IT executives fear Advanced Persistent Threat (APT) attacks
- 28% fear theft and disclosure from insiders
- 60% use either a written “honour system” security policy or have none at all
- 51% allow employees to download/install software
- Companies continue to allow employees to engage in risky behaviours!!!

# Advanced Persistent Threat

- A **long-term pattern** of sophisticated **hacking attacks** aimed at governments, companies, and political activists.

- یک الگوی طولانی مدت از حملات هکری پیچیده با هدف دولت ها ، شرکت ها و فعالان سیاسی

# Advanced Persistent Threat ...

## 1. Advanced – Full spectrum of techniques

• پیشرفته - طیف کاملی از تکنیک ها

- Not all “advanced” (e.g. malware)
- Can **develop** more advanced tools as required
- **Combines multiple targeting methods**
- Focus on **operational security** not found in less advanced threats

# Advanced Persistent Threat ...

## 2. Persistent – Priority to a specific task

• ماندگار - اولویت خاص

- **Not** opportunistically seeking information for **financial gain**
- A “**low-and-slow**” approach is typical
- Maintain **long-term access** to the target

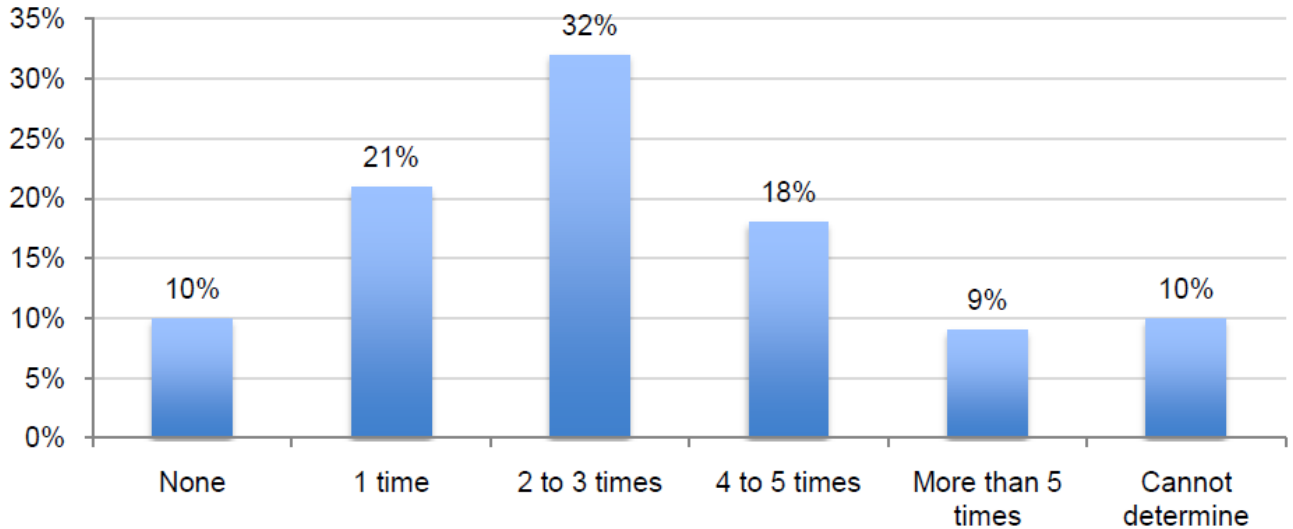


# Advanced Persistent Threat ...

## 3. Threat – Capability and intent

- تهدید - توانایی و قصد
- Executed by **coordinated human actions** vs. automation
- **Specific objective** with **skilled, motivated, organized and well funded entities**

# Multiple Successful Attacks



Perceptions About Network Security  
Survey of IT and IT security  
practitioners in the U.S. Ponemon  
Institute Research Report

583 US IT practitioners  
Average experience 9.5 years  
51% in organizations > 5000  
employees

# The Impact of Data Breaches on Reputation & Share Value

Ponemon Institute surveyed:

# 448

individuals in IT operations and information security (hereafter referred to as IT practitioners)

# 334

senior-level marketers and corporate communication professionals (hereafter referred to as CMOs)

# 549

Consumers



**Sixty-two percent** of consumers say in the past two years they have been notified by a company or government agency that their personal information was lost or stolen as a result of one or more data breaches.

# Stock Prices Drop



بلافاصله پس از افشای رخنه این شرکتها، متوسط کاهش قیمت سهام 5٪ را تجربه کردند.

# Brand Reputation Impact

۷۱٪ از CMOها معتقدند که بیشترین هزینه یک حادثه امنیتی از دست دادن ارزش نام تجاری است.



49٪ از متخصصان فناوری اطلاعات ، کاهش برند را بزرگترین هزینه يك حادثه امنیتی می دانند.

# Customer Trust Impact

**71%**

of Consumers

surveyed believe organizations have an obligation to control access to their information

**47%** **46%**

of CMOs

of IT practitioners

believe this is an obligation

# Additional Business Impact







# Consequences of Data Breach

- The consequences of a data breach can **ripple throughout the company** and have devastating and **long-term financial consequences**. These include reputation and customer loss, decline in revenues, loss of competitive advantage and employees' inability to be fully productive.

- عواقب رخنه امنیتی داده می‌تواند در سراسر شرکت افزایش یافته و پیامدهای مالی مخرب و طولانی مدت داشته باشد. اینها شامل از دست دادن اعتبار تجاری، مشتری، کاهش درآمدها، از بین رفتن مزیت رقابتی و ناتوانی کارکنان در تولید می‌باشد.



# Financial impact

INDUSTRY	 FINANCIAL SERVICES	 INSURANCE	 HEALTHCARE	 PHARMA
LOCATION	U.S.	U.S.	U.S.	U.S.
TURNOVER RATE	2.80%	2.99%	4.08%	3.17%
STOCK PRICE DECLINE	1.90%	5.67%	6.26%	5.10%
DAYS TO RECOVER	71	47	107	44

# Components of Data Breach Cost

## 1. Detection and Escalation ردیابی و بالابردن

- Activities that enable a company to reasonably detect the breach. Escalation activities are those necessary to report the breach to appropriate personnel within a specified time period
- فعالیت هایی که یک شرکت را قادر می سازد تا رخنه را تشخیص دهد. فعالیت هایی برای گزارش تخلف به پرسنل خاص در یک بازه زمانی مشخص .

## 2. Notification اطلاع رسانی

- Activities that enable the company to notify data subjects with a letter, outbound telephone call, e-mail or general notice that personal information was lost or stolen.
- فعالیت هایی که شرکت را قادر می سازد با نامه، تماس تلفنی، ایمیل یا اطلاع رسانی عمومی مبنی بر از بین رفتن یا سرقت اطلاعات شخصی، به افراد .

# Components of Data Breach Cost ....

## 3. Ex-post Response پاسخ پست

- **Activities to help victims** of a breach communicate with the company to ask additional questions or obtain recommendations in order to **minimise potential harms**.

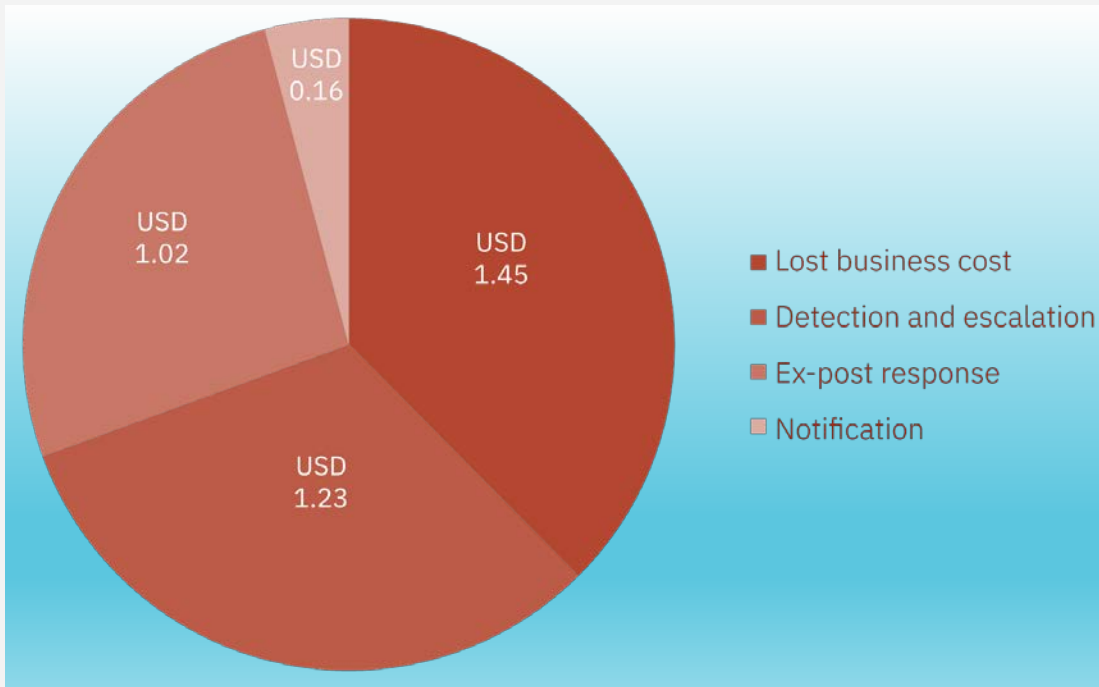
○ فعالیتهایی برای کمک به قربانیان رخنه در برقراری ارتباط با شرکت برای پرسیدن سؤالات اضافی یا دریافت توصیه هایی به منظور به حداقل رساندن آسیب های احتمالی.

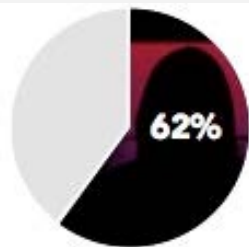
## 4. Lost business cost هزینه از دست رفته

- Activities that attempt to **minimise the abnormal loss** of customers as a result of the data breach event.

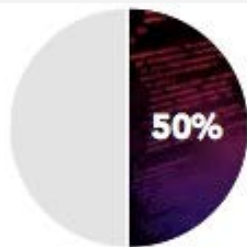
○ فعالیتهایی که سعی در به حداقل رساندن ضرر غیر طبیعی مشتریان در نتیجه رویداد رخنه در داده دارند.

# Four cost components of data breach





Consumers who  
were victims of a data  
breach



Experienced more than  
one data breach

How did the data breach affect you?

**65%**

Lost trust in organization

**31%**

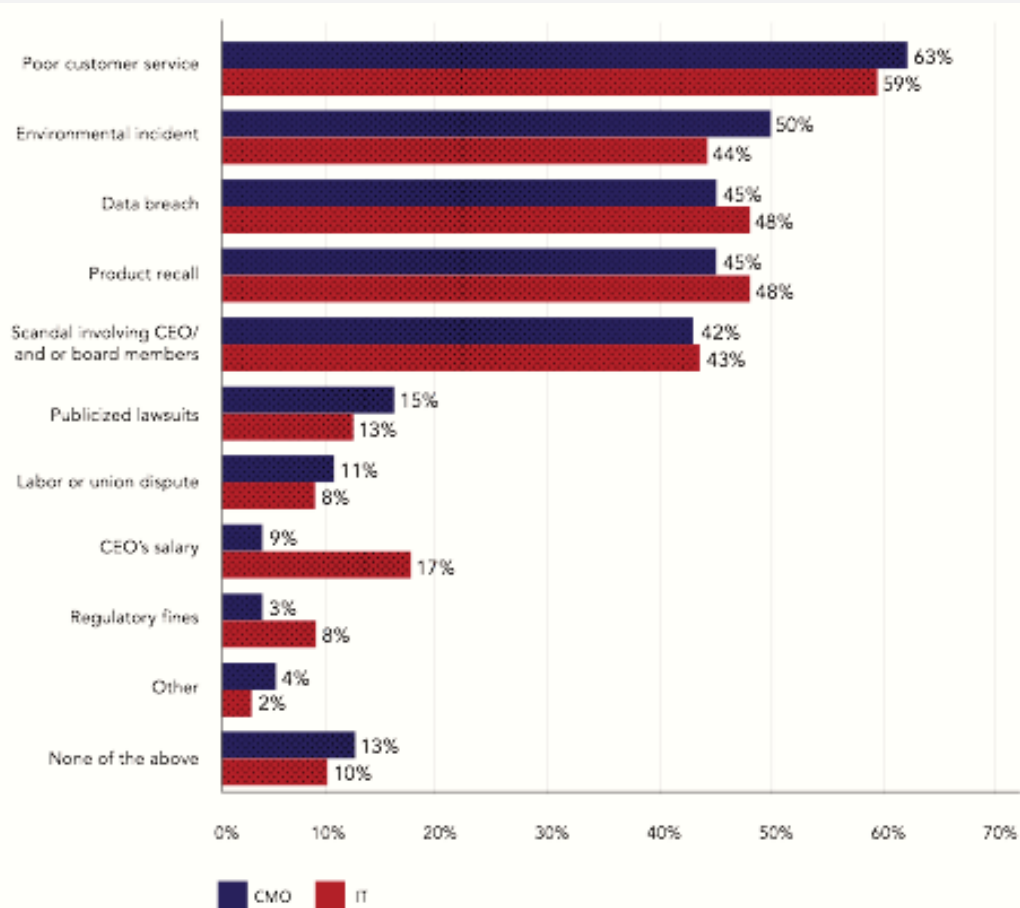
Discontinued relationship with organization

**16%**

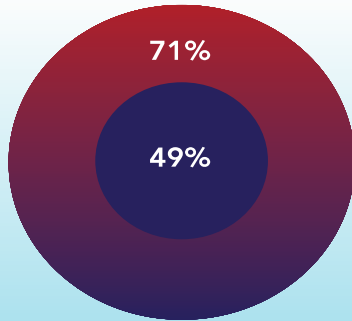
Experienced one or more criminal acts  
such as credit card fraud or identity theft

# Reputation and Brand Management

Which of the following issues would most likely have a **negative impact on your organization's reputation?**



# Perceptions about brand preservation



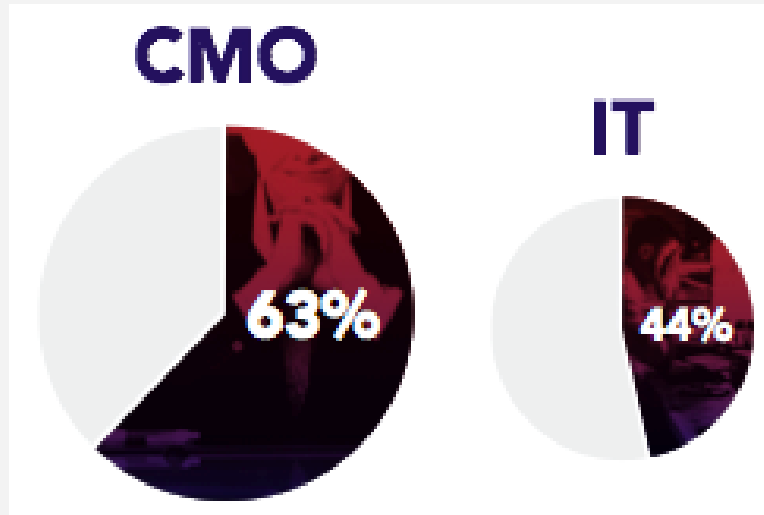
The biggest cost of a security incident is the loss of reputation and brand value



My organization invests in security in order to preserve brand or marketplace image

# Potential Blindspots and Alignment Costs

How resilient is your organization to a data breach that causes the loss or theft of high value assets?





**IDS**

**01**



# Intrusion

- Defined as an anomaly, incorrect, inappropriate activity that occurs on the network or at the host.

- به عنوان یک فعالیت ناهنجار ، نادرست ، نامناسب که در شبکه یا در هاست رخ می دهد تعریف شده است.

# Intrusion Classification

- **Attempted Break-ins** تلاش برای شکستن
- **Masquerade attacks** حملات نقاب دار
- **Penetration of Security Control Systems**
  - نفوذ در سیستم های کنترل امنیتی
- **Leakage** نشت اطلاعات
- **Denial of Service** خود داری از خدمات
- **Malicious Use** استفاده مخرب

# Anomaly

- Anomaly is a Traffic / activity that is not in accordance with the policy:
  - access from / to the forbidden host
  - has forbidden content (virus)
  - run a banned program (web directory traversal:  
GET ../../;cmd.exe)

- ناهنجاری یک ترافیک / فعالیتی است که مطابق با خط مشی نیست.

# Intrusion Detection

- Intrusion detection is the process of searching, researching, and reporting unauthorized or harmful actions of network or computer activity.
- تشخیص نفوذ، فرایند جستجو، تحقیق و گزارش اقدامات غیرمجاز یا مضر فعالیت شبکه یا کامپیوتر است.

# Need of Intrusion Detection System

- **Firewall** is the main Security System, but **Not all access through the firewall**
- There are some **applications** that are indeed **passed by a firewall** (Web, Email, etc.)
- **Not all threats come from outside the firewall**, but from within the network itself
- **Firewall is sometimes an attack object**
- Need an application as a **complement Firewall** that can **detect threats that can not be protected by the firewall**

# Why IDS is Important

- The ability to know when an intruder or attacker is engaged in reconnaissance or other malicious activity can mean the difference between being compromised and not being compromised.
- توانایی دانستن اینکه آیا یک متجاوز یا مهاجم شناسایی شده مشغول فعالیت بدخواهانه دیگری می باشد، می تواند به معنای تفاوت بین به خطر افتادن یا عیر آن باشد.

## Why IDS is Important ...

- An IDS can alert the administrator of a successful compromise, allowing them the opportunity to implement mitigating actions before further damage is caused.

- IDS می تواند مدیر را در مورد یک توافق موفقیت آمیز هشدار دهد، این امکان را برای آنها فراهم می کند تا اقدامات پیشگیرانه را قبل از ایجاد آسیب بیشتر انجام دهند.

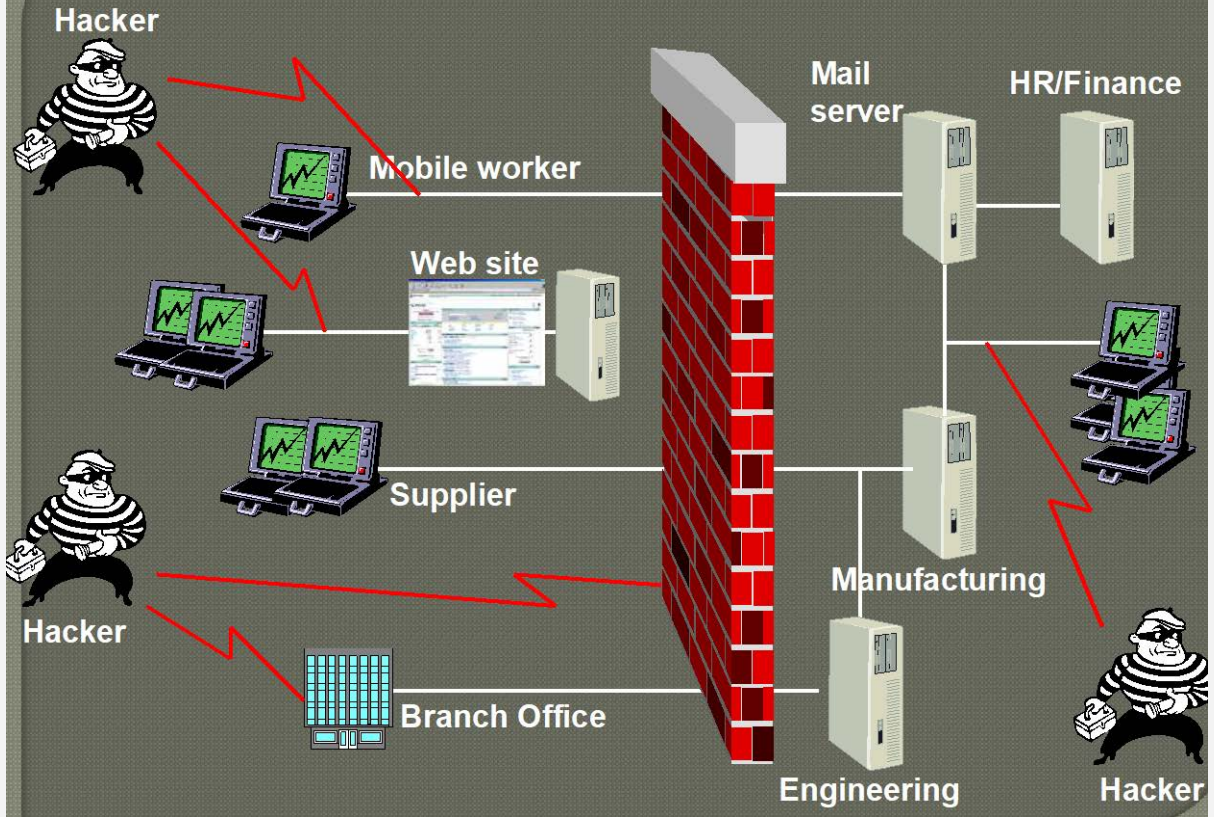


## Why IDS is Important ...

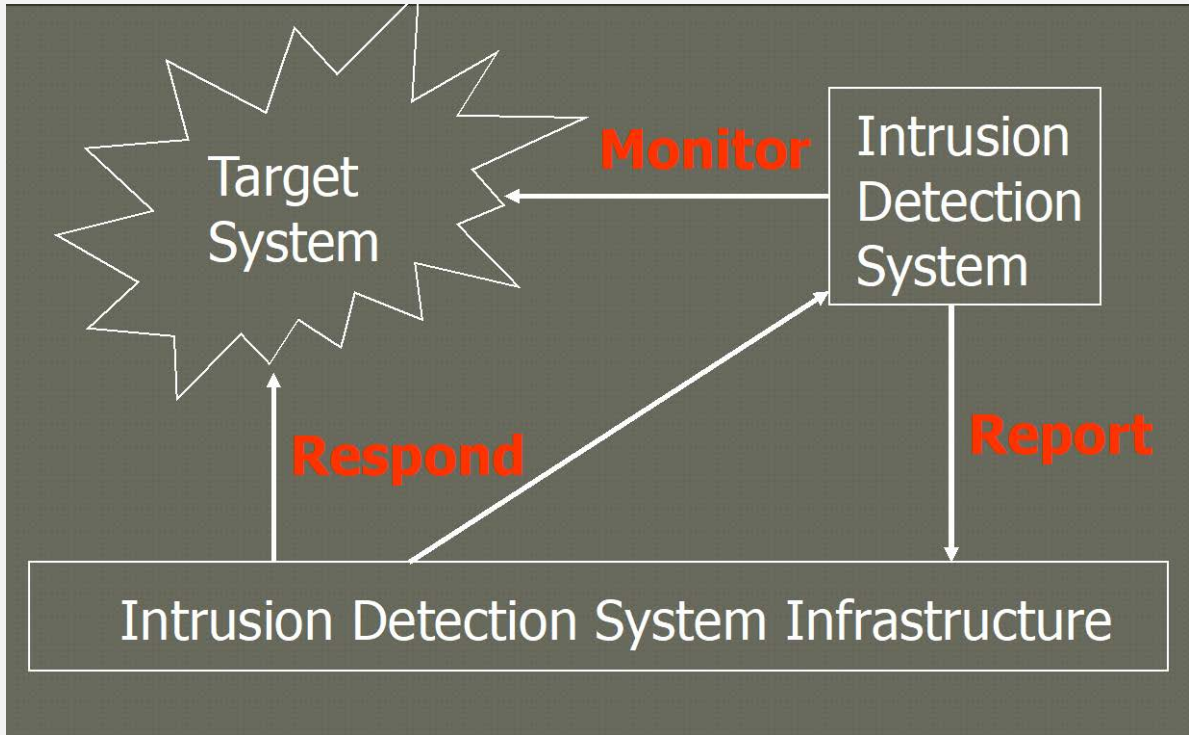
- As Corporations and other Institutions are being legally compelled to disclose data breaches and compromises to their affected customers, this can have profound effects upon a compromised company, in the way of bad press, loss of customer trust, and the effects on their stock.
- از آنجایی که شرکت ها و موسسات به طور قانونی مجبور به افشای نقض داده ها و مصالحه با مشتریان آسیب دیده خود هستند، این امر می تواند تأثیرات عمیقی بر روی اعتبار شرکت داشته باشد، فشار خبرها، از دست دادن اعتماد مشتری و تأثیرات آن بر سهام آنها.

## Internet

## Corporate Intranet



# Basic of Intrusion Detection System



# Intrusion Detection Approaches

- **Preemptory** ابتدایی
  - The Intrusion Detection tool actually listens for network traffic. When any suspicious activity is recorded, the system will take appropriate action
  - ابزار تشخیص نفوذ، در واقع ترافیک شبکه را می شنود. در صورت ثبت هرگونه فعالیت مشکوک، سیستم اقدامات مناسب را انجام می دهد.
- **Reactionary** واکنشی
  - The Intrusion Detection tool looks at the logs. When any suspicious activity is recorded, the system will take appropriate action.
  - ابزار تشخیص نفوذ، رپورت‌های مربوط را بررسی می کند. در صورت ثبت هرگونه فعالیت مشکوک، سیستم اقدامات مناسب را انجام می دهد.

# IDS Technology Based on Placement

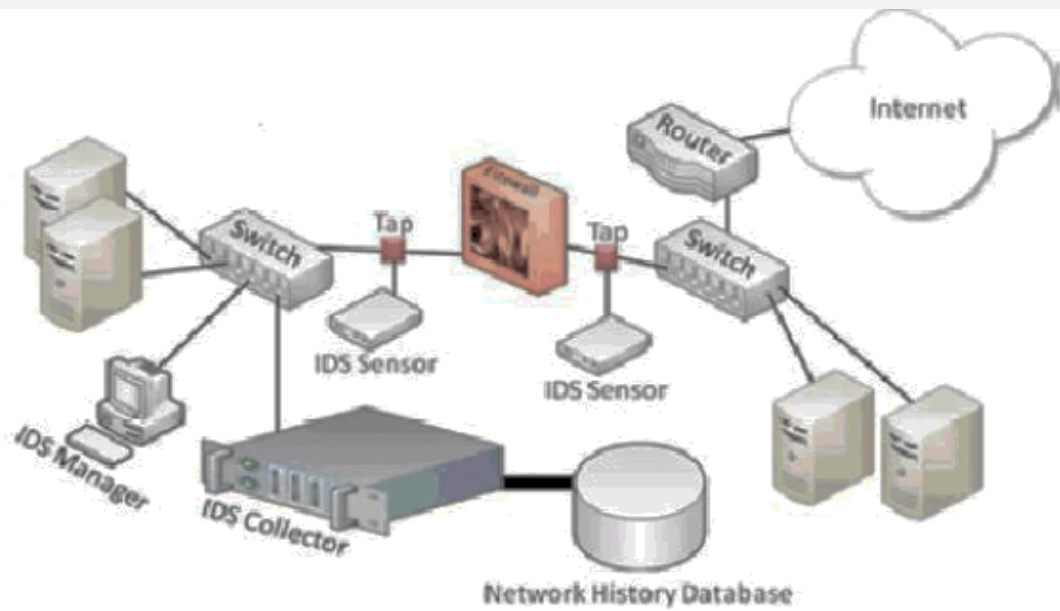
## 1. Network-based

- **Monitor** anomalies on the network, Provides real-time monitoring of network activity:
  - ✓ **Capturing, testing the header and package contents,**
  - ✓ **Compare** with the **pattern** with the **existing threat** in the database and
  - ✓ Responding if considered intruder.
- Packet monitors can be placed **outside the firewall** (detects Internet-based attacks) and **within the network** (detects internal attacks).
- Responses are: **notifying a console, sending an e-mail message, terminating the session.**
- **Tools: Snort**

# IDS Technology Based on Placement

## 2. Host-based

- **Monitor anomalies on the host, Eg. monitor logfile, process, file ownership, mode.**
- Tools:
  - ✓ Log scanners
  - ✓ Swatch
  - ✓ Log check
  - ✓ Modsecurity
  - ✓ File System Integrity Checkers
  - ✓ Tripwire



**Attack  
Detection**

**02**





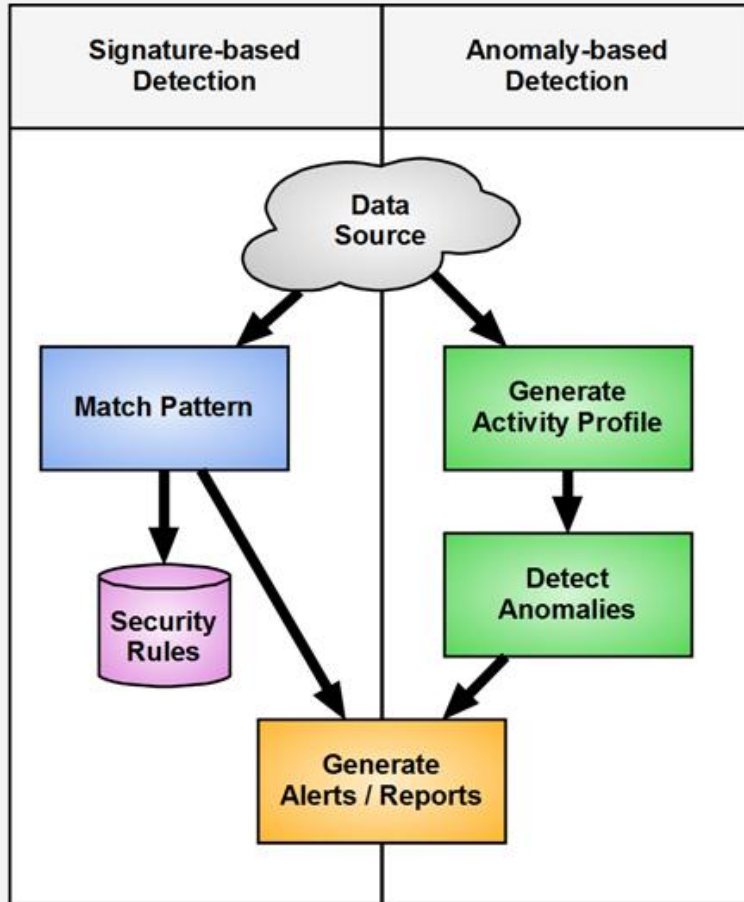
# Attack Detection Methods

- Rule-Based / Misuse-Based / Signature-Based Detection
- Anomaly-Based Detection

# Attack Detection Methods ...

- Signature-based detection:
  - detects intrusions by **monitoring network traffic and matching similar signatures.**
  - Need to **model the pattern** of various intrusions is a very **difficult** and **time-consuming** job and **can not detect any type of new intrusion that was not previously recognized.**
- Anomaly-based detection:
  - The system **defines the pattern or behavior of the previous network. All deviations from the normal pattern will be reported as an attack.**
  - Can detect new attack by seeing deviation from normal pattern.

# Attack Detection Methods ...



# Anomaly-Based Detection

- First of all network traffic data is captured with tcpdump software.
- After going through the preprocessing phase, the data is divided into two parts namely **data training** and **data testing**.
- Using a particular method of training data is classified into two classes of **intrusion** and **non intrusion**.
- Training results are used to perform testing.

Aspects	Anomaly Detection	Misuse Detection
Characteristics	Uses the deviation from normal usage patterns to identify intrusions.	Uses the patterns of known attacks (signatures) to identify intrusions.
Drawbacks	<ul style="list-style-type: none"> <li>- Has to study sequential interrelation between transactions</li> <li>- False positives.</li> </ul>	<ul style="list-style-type: none"> <li>- Known attacks have to be hand-coded</li> <li>- Unable to detect new attacks</li> <li>- Need signatures update</li> <li>- False negatives</li> </ul>

# Thresholds

- Threshold is a value that represents the boundary of normal activity.
- آستانه مقداری است که مرز فعالیت طبیعی را نشان می دهد.
- Example: Maximum three tries for login
- Common thresholds:
  - ❖ File I/O Activity
  - ❖ Network Activity
  - ❖ Administrator Logins and Actions

# Thresholds ...

- **A rule tells the IDS which packets to examine and what action to take.**
- Similar to a firewall rule:
  - Alert tcp any any -> 192.168.1.0/24 111  
(content:"|00 01 86 a5|";msg:"mountd access");**
  - Alert: specifies the action to take
  - Tcp: specifies the protocol
  - Any any 192.... : specifies the source and destination within the given subnet.
  - 111: specifies the port
  - Content: specifies the value of a payload
  - Msg: specifies the message to send

**Issues of  
IDS**

**03**





# Issues of IDS

- An IDS is sensitive to configuration.
- Possible types of IDS errors:
  - **False positive** (unauthorized user let in)
    - مثبت کاذب (کاربر غیر مجاز اجازه ورود می دهد)
  - **False negative** (authorized user denied access)
    - منفی کاذب (دسترسی مجاز به کاربر مجاز نیست)
  - **Subversion error** (compromised the system from detecting intrusion)
    - خطای براندازی (سیستم را از تشخیص نفوذ به خطر می اندازد)

# False Negatives

- When an IDS fails to detect an attack.
- هنگامی که IDS نتواند حمله را تشخیص دهد.
- False negatives occur when:
  - The **pattern of traffic is not identified** in the **signature database**, such as **new attack patterns**.
- False negatives are deceptive because you usually have **no way of knowing** if and when they occurred.
- You are most likely to identify false negatives when an **attack is successful and wasn't detected by the IDS**.

# False Positives

- Described as a false alarm.
- به عنوان هشدار دروغین توصیف شده است.
- When an **IDS mistakenly reports** certain “normal” network activity as malicious.
- **Administrators** have to fine **tune the signatures** or **heuristics** in order to **prevent** this type of problem.

# Subversion Error

- A subversion error occurs when **an intruder modifies** the operation of the intrusion detector to **force false negatives to occur**.
- **More complex** and tie in with false negative errors.
- An intruder could use **knowledge** about the internals of an intrusion detection system to **alter its operation**, possibly allowing anomalous behavior to proceed.
- The intruder could then **violate the system's operational security constraints**.
- This may be discovered by a human operator examining the logs from the intrusion detector, but it would appear that the intrusion detection system still *seems to be working correctly*.

# IDS Pros

- Can **detect external hackers**, as well as, **internal network-based attacks**.
- **Scales** easily to provide protection for the entire network.
- Offers **centralized management** for correlation of distributed attacks
- Provides **defence in depth**.  
Gives **administrators** the ability to **quantify attacks**.
- Provides an **additional layer of protection**.

# IDS Cons

- Generates **false positives and negatives**
- **Reacts to attacks** rather than preventing them
- **Requires full-time monitoring** and highly skilled staff dedicated to interpreting the data.
- Requires a **complex incident response process.**
- **Cannot monitor traffic at higher network traffic rates.**
- Generates an **enormous amount of data to be analysed.**
- It is expensive.

**Intrusion  
Prevention  
System  
(IPS)**

**04**



# Intrusion Prevention System (IPS)

- An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

- سیستم پیشگیری از تهاجم (IPS) یک فناوری امنیتی / پیشگیری از تهدید شبکه است که جریان‌های ترافیک شبکه را برای شناسایی و جلوگیری از سوء استفاده از آسیب پذیری بررسی می‌کند.



## IPS ...

- Vulnerability exploits usually come in the form of **malicious inputs** to a target application or service that **attackers use to interrupt and gain control** of an application or machine.
- Following a **successful exploit**, the attacker can disable the target application (resulting in a **denial-of-service** state), or can potentially **access** to all the rights and permissions available to the compromised application.

## IPS ...

- The IPS often sits **directly behind the firewall** and provides a complementary layer of analysis that negatively selects for dangerous content.
- Unlike its predecessor the **IDS**—which is a **passive** system that scans traffic and reports back on threats—the **IPS is placed inline** (in the **direct communication path between source and destination**), **actively analyzing** and taking automated actions on all **traffic flows** that enter the network.

# IPS Actions

- Sending an alarm to the administrator (as would be seen in an IDS)
- Dropping the malicious packets
- Blocking traffic from the source address
- Resetting the connection

**Thanks for your Attention.**