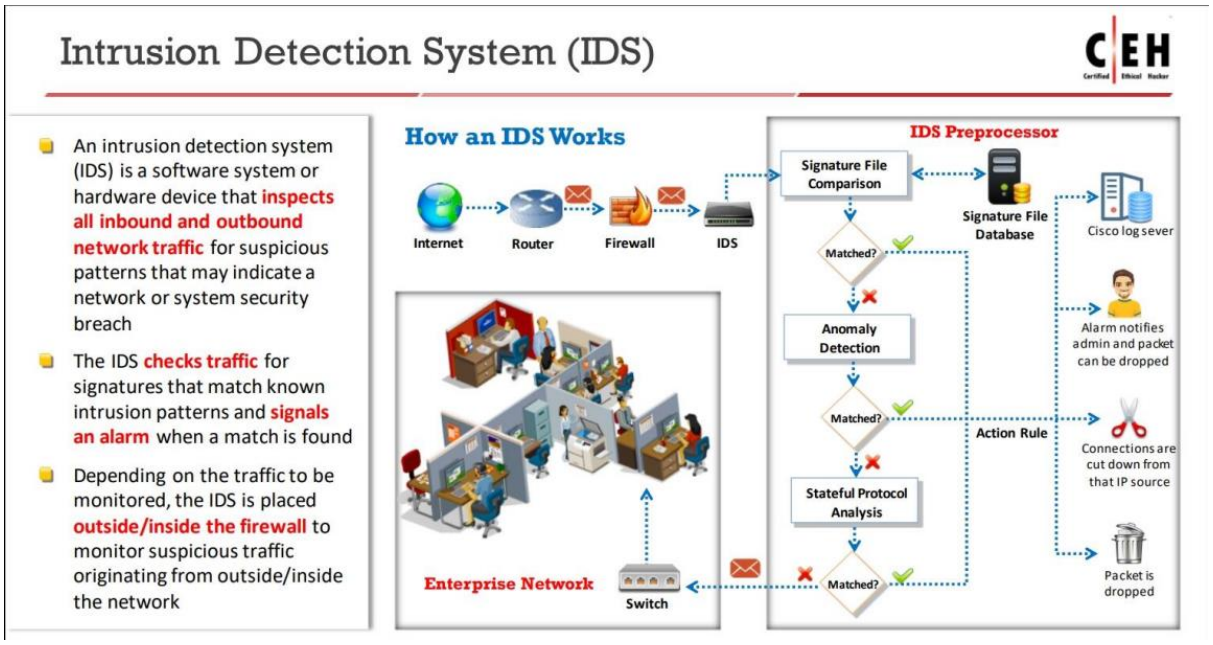
Evading IDS, Firewalls and honeypots

Intrusion Detection System

An Intrusion Detection System (IDS) is a software or device that monitors a network or system for malicious activity or policy violations. IDS deploys near the firewall depending on the traffic to be monitored an IDS is placed outside/inside the firewalls to monitor the traffic It can alert the administrator but cannot prevent action to any damage or further intrusion. It can improve the security posture of an organization by detecting and preventing attacks.

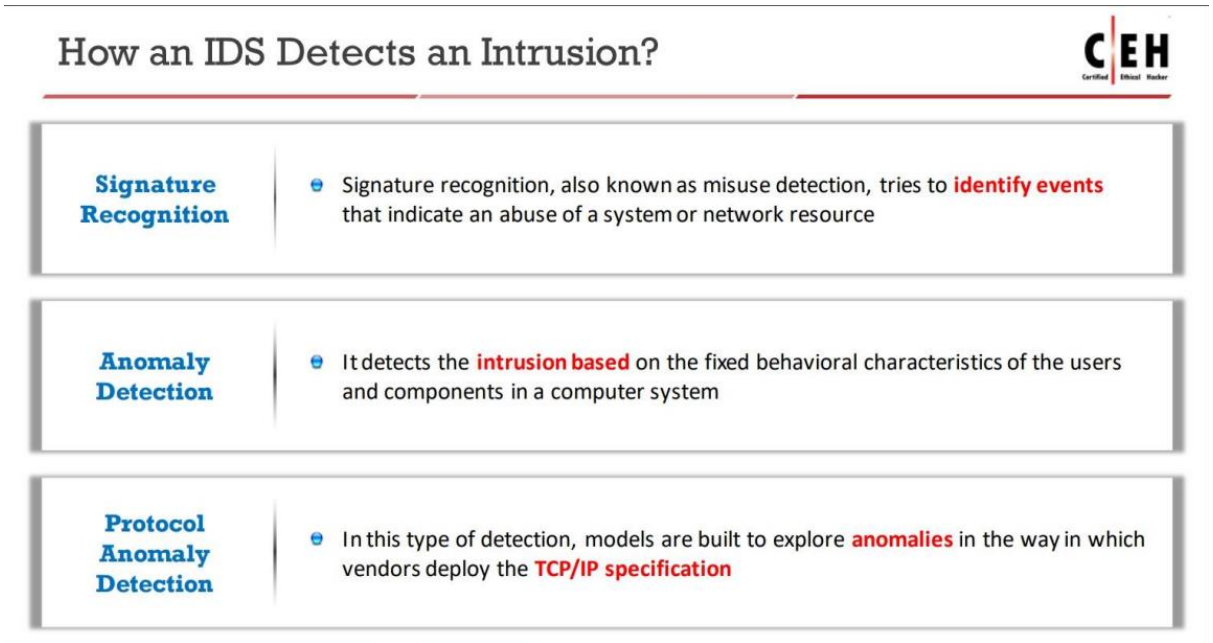


How IDS detect an Intrusion

1) Signature recognition - These are systems that monitor network or system activity and compare it to a database of known attack signatures or indicators of compromise (IOCs). If a match is found, the system alerts the administrator or takes action to prevent or mitigate the attack.

2) Anomaly Detection - It works by creating a baseline of normal network behaviour and comparing the current activity to the baseline.

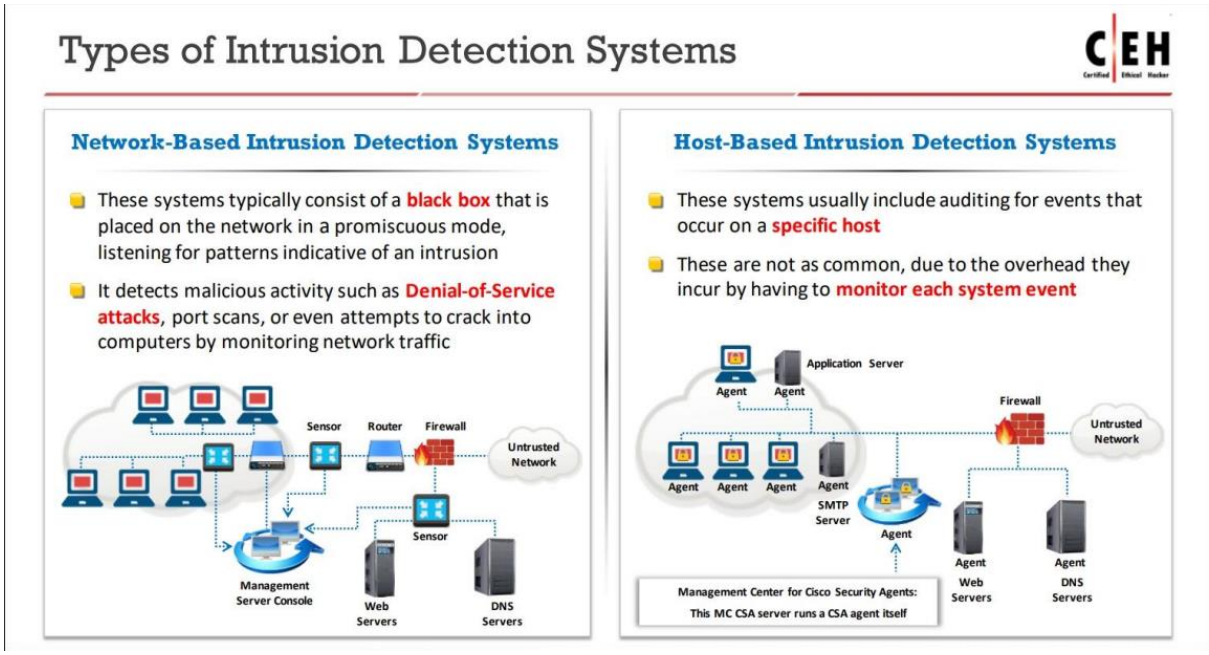
3) Protocol Anomaly Detection - Any deviation from the baseline is considered an anomaly and is flagged as a potential intrusion. It can adapt to changing network conditions and learn from new data.



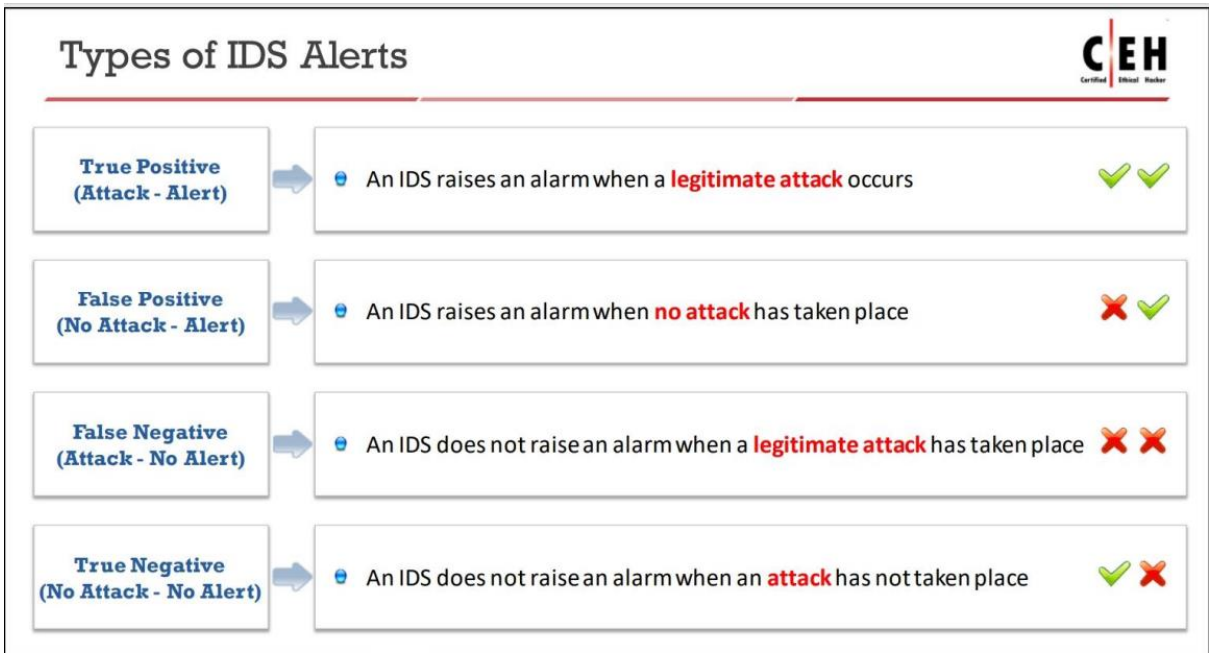
Types of Intrusion Detection System

1) Network - Based Intrusion detection system - A network-based intrusion detection system (NIDS) is a type of security system that monitors and analyses the traffic on a network for any signs of malicious or suspicious activity. A NIDS can detect and alert the administrator of various threats, such as denial-of-service attacks, port scans, malware infections, or unauthorized access attempts.

2) Host - Based Intrusion detection system - A HIDS works by capturing the data and events that occur on the host, such as system calls, file accesses, network traffic, or user actions, and comparing them to a set of rules or signatures that define known attacks or anomalies. If a match is found, the HIDS generates an alert or a log entry that can be reviewed by the administrator or another security tool. A HIDS can also perform statistical analysis or machine learning to detect abnormal patterns or behaviours in the host data.



Types of IDS Alerts



True Positive --> Attack - Alert ✅✅

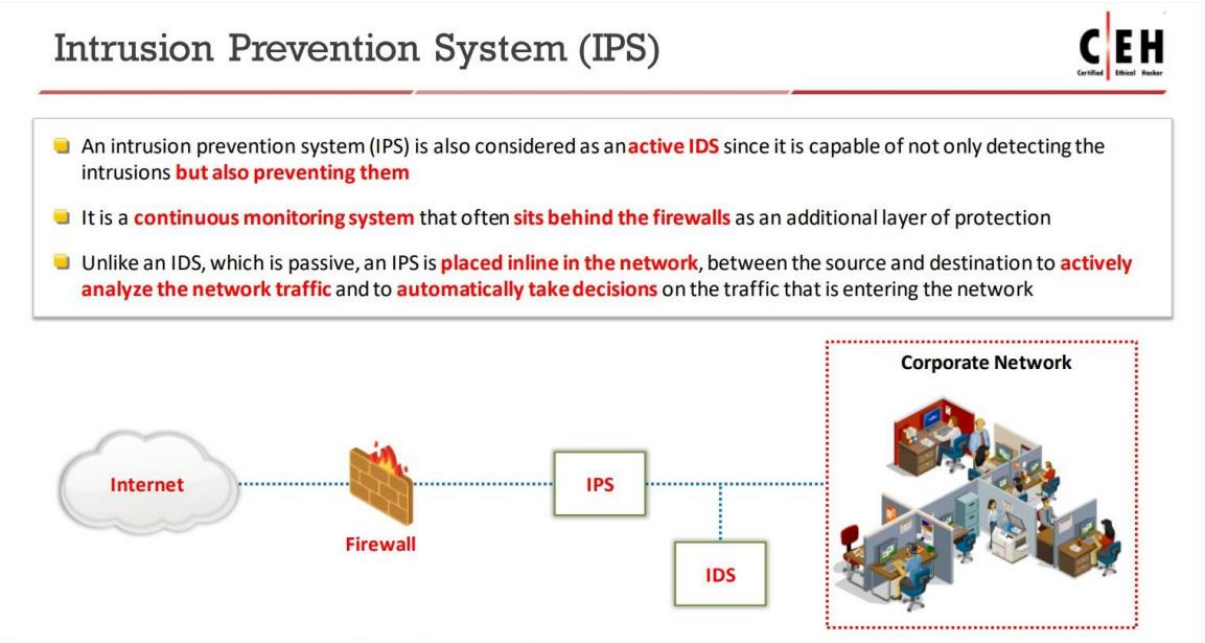
False Positive --> No Attack - Alert ❌✅

False Negative --> Attack - No Alert ❌❌

True Negative --> NO Attack - No Alert ✅❌

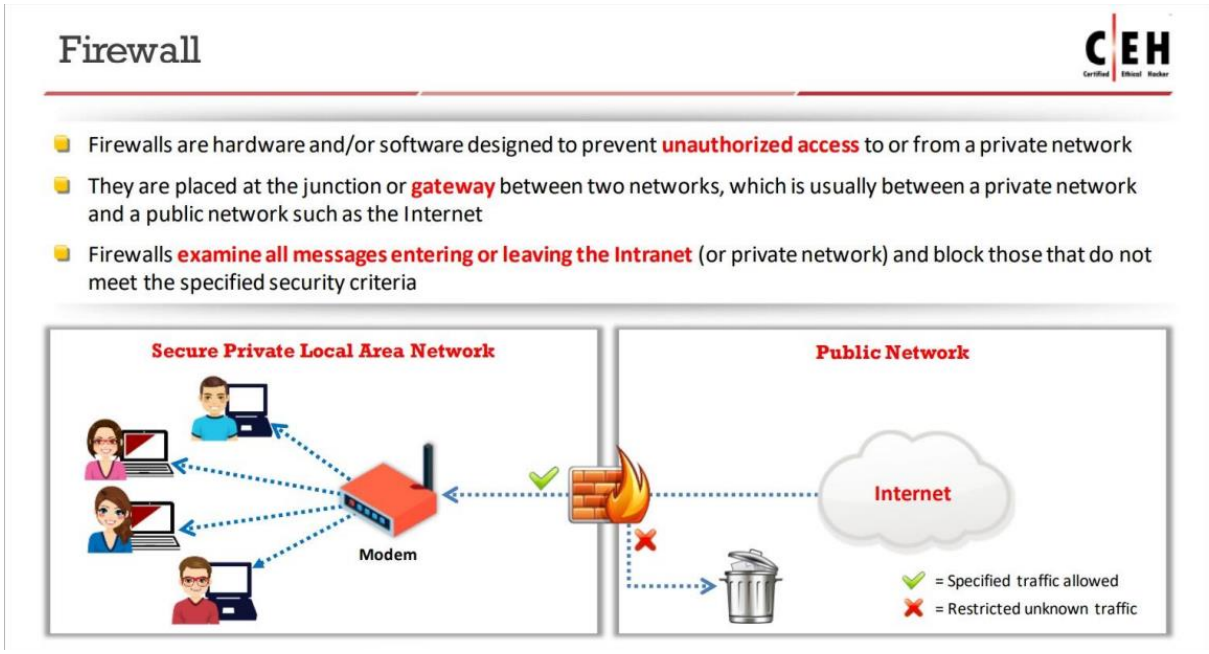
Intrusion Prevention System

An Intrusion Prevention System (IPS) is a type of network security device that monitors and analysis the traffic on a network for any signs of malicious or suspicious activity. It can also take action to block or prevent the detected threats from harming the network or its resource.



Firewalls

Firewalls are network security devices or software programs that monitor and filter the traffic between different networks or hosts. They can block or allow data packets based on a set of rules or criteria, such as the source, destination, protocol, or content of the packets.



Firewalls Types

Packet-filtering - Firewalls that only look at headers.

Stateful (Dynamic Packet Filtering) - Layer 3 + 4 (Network + Transport layer)

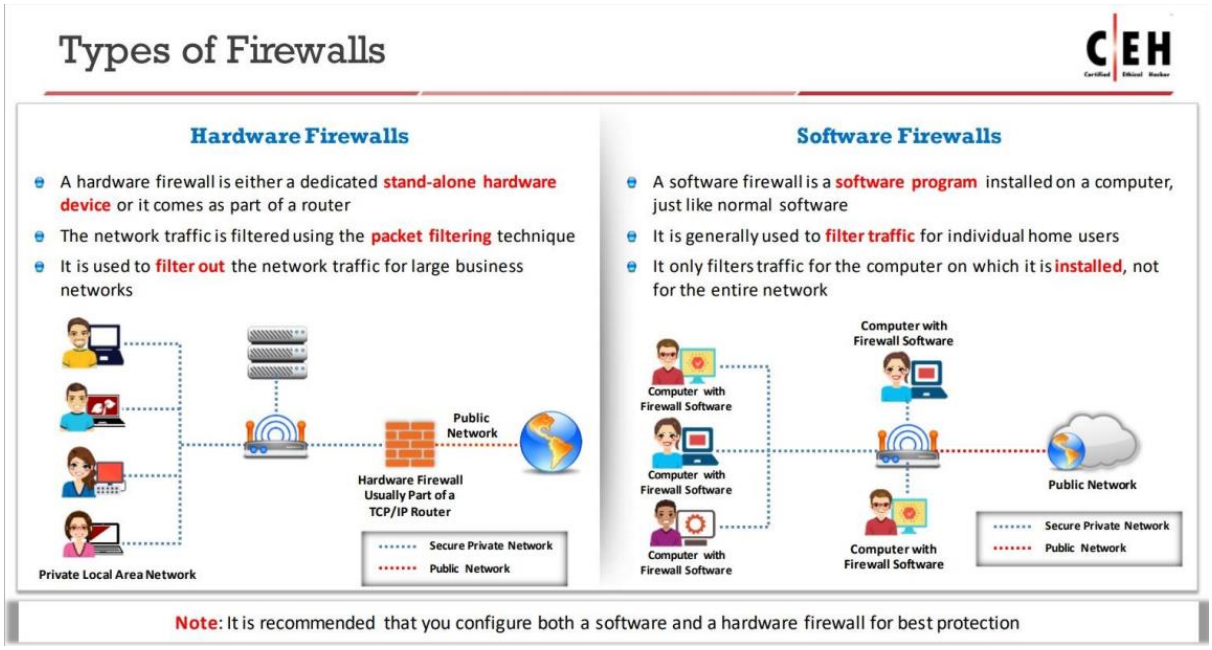
Stateless (Static Packet Filtering) - Layer 3 (Network)

Deep Packet Inspection - Layer 7 (Application Layer)

Types of Firewalls

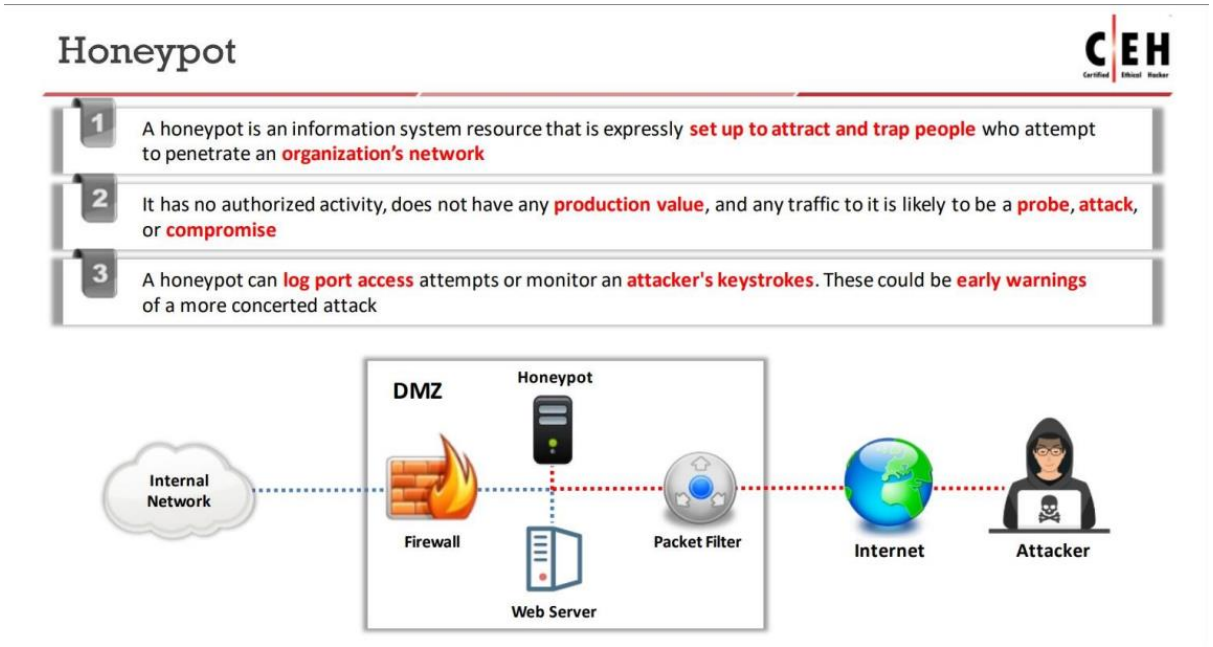
1) Hardware Firewalls – A hardware firewall is a dedicated firewall device placed on the perimeter of the network. It is an integral part of the network setup and is also build into broadband networks or used as a standalone product. It employs the technique of packet filtering.

2) Software Firewalls – A software firewall is similar to a filter. It sits between a regular application and networking components of the OS. It is more useful for individual home users and it is suitable for mobile users who need digital security when working outside the cooperate network.



Honeypot

Honeypots are decoy systems or servers deployed alongside production systems within your network. When deployed as enticing targets for attackers, honeypots can add security monitoring opportunities for blue teams and misdirect the adversary from their true target.



Types of Honeypots

1) Low -Interaction Honeypots - Low-interaction honeypots are less resource-intensive and gather rudimentary information regarding the kind of threat and where it came from. These are relatively simple to set up, and they make use of Transmission Control Protocol (TCP), Internet Protocol (IP), and network services. However, there is nothing inside the honeypot to hold the attacker's attention for a considerable amount of time.

2) Medium -Interaction Honeypots – Mid-interaction honeypots imitate elements of the application layer, but they do not have an operating system. Their mission is to confuse an attacker or stalk them so the organization has more time to ascertain how to react to the kind of attack in question.

3) High -Interaction Honeypots – A high-interaction honeypot is designed to get attackers to invest as much time as possible inside the honeypot. This gives the security team more opportunities to observe the targets and intentions of the attacker and more chances to discover vulnerabilities within the system.

4) Pure Honeypots - A pure honeypot refers to a full-scale system running on various servers. It completely mimics the production system. Within a pure honeypot is data made to look confidential, as well as "sensitive" user information, which have a number of sensors used to track and observe attacker activity.

Types of Honeypots

Classification of honeypots based on their design criteria:

Low-interaction Honeypots	These honeypots simulate only a **limited number of services** and applications of a target system or network
Medium-interaction Honeypots	These honeypots simulate a **real operating system**, applications, and services of a target network
High-interaction Honeypots	These honeypots **simulate all services** and applications of a target network
Pure Honeypots	These honeypots emulate the **real production network** of a target organization

Classification of honeypots based on their deployment strategy:

- Production Honeypots
- Research Honeypots

Classification of honeypots based on their deception technology:

- Malware Honeypots
- Spam Honeypots
- Spider Honeypots
- Database Honeypots
- Email Honeypots
- Honeynets

Honeynet

Two or more honeypots on a network form a honeynet. Honeynets and honeypots are usually implemented as parts of larger Network Intrusion Detection Systems.

IDS Evasion Techniques

Insertion Attack and Evasion

Insertion Attack

- Insertion is the process by which the **attacker confuses the IDS** by forcing it to read invalid packets
- An IDS blindly believes and accepts a packet that an end system rejects, and an attacker exploits this condition and **inserts data into the IDS**
- This attack occurs when the **NIDS is less strict** in processing packets than the internal network
- The attacker obscures extra traffic and the IDS concludes that the traffic is harmless. Hence, the **IDS gets more packets** than the destination
- An attacker sends one-character packets to the target system via the IDS with **varying TTL** such that some packets reach the IDS but not the target system

Evasion

- In this evasion technique, an end system **accepts a packet** that an IDS rejects
- Using this technique, an attacker **exploits the host computer** without the IDS ever realizing it
- The attacker sends **portions of the request** in packets that the IDS mistakenly rejects, allowing the removal of parts of the stream from the IDS
- For example, if the malicious sequence is sent **byte-by-byte** and one byte is rejected by the IDS, the IDS cannot detect the attack
- Here, the **IDS gets fewer packets** than the destination