INTRUSION DETECTION SYSTEMS

Paper Referred to -
https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7

After the firewall, there are mainly two types of systems.

- Intrusion Detection Systems (IDS)
  This detects any sort of intrusion and alerts the terminal.
- Intrusion Prevention Systems (IPS)
  The IPS does everything IDS does and a little more.

Intrusion is defined as – Any type of unauthorized activity which might pose a threat to an information system.

Based on the methods used to identify the intrusion, IDS can be broadly classified into two different groups.

- SIDS – Signature-Based Intrusion Detection Systems
- AIDS – Anomaly-Based Intrusion Detection Systems

SIDS

SIDS is used to identify an intrusion based on pattern matching. When an intrusion is detected, the system tries to match the signature of the attack with the one present in the signatures database. If a match is found, then an alert is generated. SIDS is very effective when dealing with previously known attacks. But is not very effective in the case of zero-day attacks and modern-day malware whose signature usually spans across various packets. To overcome these difficulties, AIDS is used.

AIDS

In AIDS, a normal model of a computer is created using ML techniques, any deviation from this normal model is considered an intrusion. AIDS is now particularly useful because not only does it alert better but alerts are generated even after the attacker has entered the machine as a malicious activity is very different from normal user behaviour. Due to this feature, AIDS, unlike SIDS can detect zero-day attacks.

Based on the technology used IDS can be classified into –

- HIDS - Host-Based Intrusion Detection System
- NIDS – Network-Based Intrusion Detection System

HIDS

HIDS inspects the data coming from the host and other sources such as the OS, server logs, firewall etc. HIDS is used for detecting insider attacks which include network traffic.

NIDS

This monitors the traffic which is extracted from a network using packet capture. NIDS monitors all computers in each network.

Statistics-Based Techniques

Statistics-based IDS uses the concepts of mean, median, and mode to identify the differences between normal and unusual behaviour, instead of scanning each packet passing through the network. This has a rather high error rate as the activities considered anomalous may be genuine. This is because the IDS is statistics based and lacks a well defines taxonomy.

Time Series Model

Observations are made over a time interval instead of inspecting each packet and any new observation is considered an anomaly if the frequency of recurrence is too low.

Knowledge-Based Techniques

This is also known as the expert systems method. This process generates a knowledge base which reflects a legit traffic profile, any deviation from the same is considered an anomaly. The biggest disadvantage to this model is that the normal model is generated based on human knowledge and hence it has to be constantly updated.
Some types of knowledge-based models are – Finite State Models, description language, expert systems, and signature analysis.

AIDS-BASED MACHINE LEARNING TECHNIQUES

For pattern detection and normal model training, different machine learning techniques such as Supervised Learning, Unsupervised Learning, and Semi-

Supervised learning can be used and existing datasets of DARPA etc can be used to train the model.

FEATURE SELECTION

1. Wrapper Methods - This makes subgroups of variables, to study how they are interrelated.
   Drawback - Small amount of Data - Accumulative Overfitting
   A large amount of Data-Large Calculation Time.

2. Filter Methods – Features are nominated based on their scores in several statistical tests. These methods are usually applied in the pre-processing stage.

TYPES OF COMPUTER ATTACKS

Every cyber-attack can be broadly classified under one of the 4 following categories.
DDOS, Probing Attacks, User to Root (U2R), Remote to Local (R2L).

IDS EVASION TECHNIQUES

- Fragmentation – A data packet is divided into several smaller packets. These fragmented packets are then re-assembled at the recipient. Then it is sent to the application layer of the network. Here, the packets must be reconstructed as they were at the fragmentation point. This assembly and de-assembly require holding the packet in the memory.

- Flooding – The attacker overwhelms the detector by sending a lot of traffic at once. This causes a failure in the detector. This is not an attack but is a cover for the actual attack.

- Obfuscation – To avoid detection, the message is made extremely difficult to understand. A good IDS must have hexadecimal strings in it so that the malware can be detected no matter how it's encoded.

- Encryption – Attacks on encrypted protocols cannot be read by the IDS. The encrypted traffic cannot be matched against any existing database of signatures, thereby making it difficult to examine.