**ETHICAL HACKING**

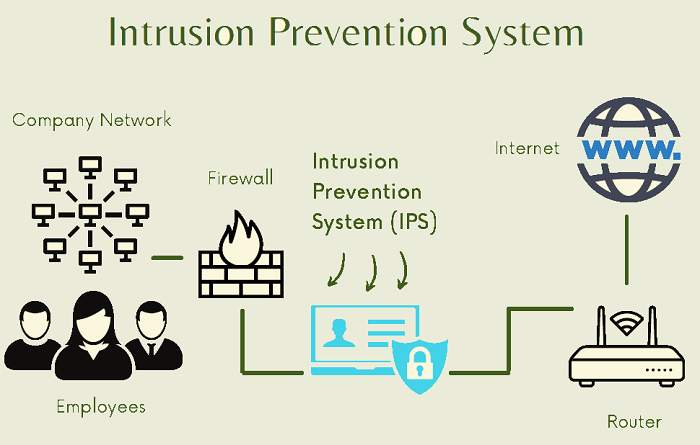
**ASSIGNMENT -3**

Name : Srivishali K

Reg.No: 19IT104

**INTRUSION DETECTION SYSTEMS :**

The purpose of an intrusion detection system (IDS) is to protect the confidentiality, integrity, and availability of a system. Intrusion detection systems (IDS) are designed to detect specific issues, and are categorized as signature-based (SIDS) or anomaly-based (AIDS). IDS can be software or hardware.

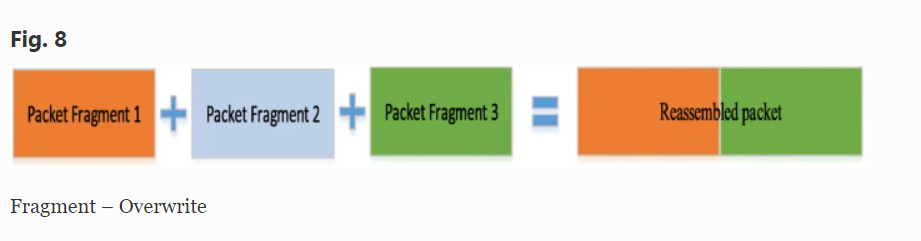


**IDS evasion techniques :**

Cybercriminal may use to avoid detection by IDS such as Fragmentation, Flooding, Obfuscation, and Encryption. These techniques pose a challenge for the current IDS as they circumvent existing detection methods.

**Fragmentation**

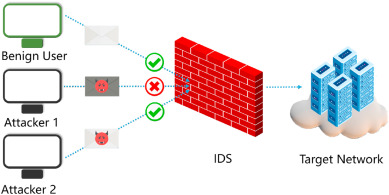
A packet is divided into smaller packets. The fragmented packets are then be reassembled by the recipient node at the IP layer before forwarding it to the Application layer. To examine fragmented traffic correctly, the network detector needs to assemble these fragments similarly as it was at fragmenting point. The restructuring of packets needs the detector to hold the data in memory and match the traffic against a signature database. Methods used by attackers to escape detection by hiding attacks as legitimate traffic are fragmentation overlap, overwrite, and timeouts (Ptacek & Newsham, 1998; Kolias et al., 2016). Fragmentation attack replaces information in the constituent fragmented packets with new information to generate a malicious packet.



The duration of time that the detector can maintain a state of traffic might be smaller than the period that the destination host can maintain a state of traffic .The malware authors try to take advantage of any shortcoming in the detection method by delivering attack fragments over a long time.

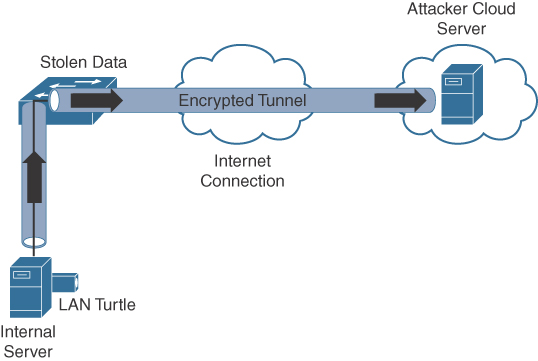
**Flooding**

The attacker begins the attack to overwhelm the detector and this causes a failure of control mechanism. When the detector fails, all traffic would be allowed . A popular method to create a flooding situation is spoofing the legitimate User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP). The traffic flooding is used to disguise the abnormal activities of the cybercriminal. Therefore, IDS would have extreme difficulty to find malicious packets in a huge amount of traffic.



**Obfuscation**

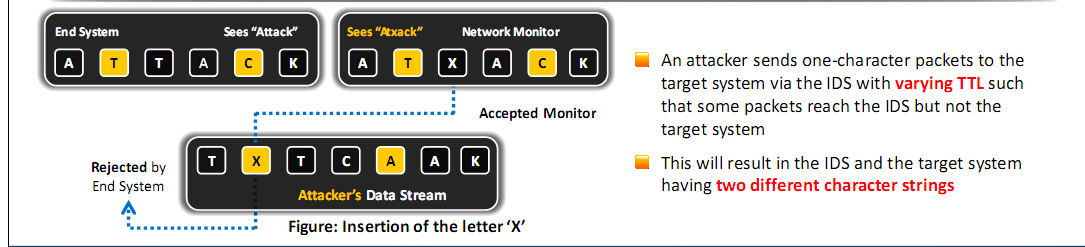
Obfuscation techniques can be used to evade detection, which are the techniques of concealing an attack by making the message difficult to understand. The terminology of obfuscation means changing the program code in a way that keeps it functionally identical with the aim to reduce detectability to any kind of static analysis or reverse engineering process and making it obscure and less readable. This obfuscation of malware enables it to evade current IDS.



Obfuscation attempts to utilize any limitations in the signature database and its capability to duplicate the way the computer host examines computer's data .An effective IDS should be supporting the hexadecimal encoding format or having these hexadecimal strings in its set of attack signatures .Unicode/UTF-8 standard permits one character to be symbolized in several various formats. Cybercriminals may also use double-encoded data, exponentially escalating the number of signatures required to detect the attack.

**Insertion Attack**

* 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 the attacker exploits this condition and inserts data into the IDS
* Occurs when NIDS is less strict in processing packets than the internal network
* The attacker obscures extra traffic and IDS concludes the traffic is harmless
* The IDS gets more packets than the destination
* IDS and the end system construct two different strings IDS Insertion



False Positive Generation

* Craft malicious packets just to generate alerts
* These packets generate a large number of false positive alerts
* False positives are used to hide the real attack traffic
* Makes it difficult to differentiate the attack traffic with the false positives

**Session Splicing**

* Attacker splits the attack traffic into many packets
* It is effective against IDS that do not reconstruct packets before checking them against intrusion signatures
* If attackers are aware of delay in packet reassembly at the IDS the can add delay between packet transmissions to bypass the reassembly