Packet-Mistreating Attacks

In these types of attacks the compromised router mishandles or mistreats packets, resulting in congestion. These attacks are difficult to detect. They have limited effectiveness when compared to routing table poisoning and DoS attacks because the attacks are confined to only a part of the network rather than the whole network.

Attackers carrying out packet-mistreating attacks often acquire an actual data packet and mistreat it. The mistreated packet could invoke the following problems:

- **Denial of service**: This can be caused indirectly by directing an irrepressible number of packets to the victim's address, thus rendering the victim router and its network inaccessible for regular traffic.
- **Congestion**: This is caused by misrouting packets to heavily loaded links of a network.
- **Lowering of connection throughput**: The attacker carrying out a packet-mistreating attack can decrease throughput by preventing TCP packets from broadcasting further. The victim router, sensing congestion, would lower the sending speed, resulting in a decrease in connection throughput.

Routing Table Poisoning

Routing table poisoning is one of the most prominent types of attacks. When an attacker maliciously alters, or poisons, a routing table, the routing-data update packets are also maliciously modified. These routing-data packets are needed by some routing protocols to broadcast their IP packets. Misconfigured packets produce false entries in the routing table, such as a false destination address. This leads to a breakdown of one or more systems on a network and the following problems:

- **Suboptimal routing**: This attack affects real-time applications on the Internet.
- **Congestion**: This attack can lead to artificial congestion, which cannot be eliminated using conventional congestion control methodologies.
- **Partition**: Due to the presence of false entries in the routing table, artificial partitions are created in the network.
- **Overwhelmed host**: The compromised router can be used as a tool for DoS attacks.
- **Unauthorized access to data**: The attacker can access the data present in the compromised network.

Hit-and-Run Attacks

Hit-and-run attacks occur when an attacker injects a small number of bad packets into the router to exploit the network.

This type of attack is similar to a test attack because the attacker gains knowledge of whether the network is online and functioning. This kind of test attack, however, can cause long-term damage and is hard to detect.

Persistent Attacks

In a persistent attack, the attacker continuously injects bad packets into the router and exploits the vulnerabilities that are revealed during the course of the injection process.

These attacks can cause significant damage because the router can get flooded with packets and cease functioning due to the constant injection of packets. These attacks are comparatively easy to detect.

Router Forensics Versus Traditional Forensics

Router forensics does not differ much from traditional forensics except in some particular steps taken during investigations. During router investigations, the system needs to be online, whereas in traditional forensic investigations, the system needs to be powered off. The system must be online so the forensic investigator can have exact knowledge of what type of traffic flows through the router.

In traditional forensics, the system is powered off because data may get erased or modified by the intruder and the forensic investigator may be unable to discover what kind of data has been modified. Data remains constant, unchanged, and ineffective during router investigations because it is prohibited for any other person to handle or read the data.

In traditional forensics, a copy of the data to be investigated should be made for examinations, since the data is most likely to be modified or erased.