CenterTrack Method

An overlay network is a supplemental or auxiliary network that is created when a collection of nodes from an existing network are joined together using new physical or logical connections to form a network on top of the existing one. The first step in the CenterTrack approach is to create an overlay network, using IP tunnels to connect the edge routers in an ISP’s network to special-purpose tracking routers that are optimized for analysis and tracking. The overlay network is also designed to further simplify hop-by-hop tracing by having only a small number of hops between the edge routers. In the event of a DoS flood attack, the ISP diverts the flow of attack packets from the existing ISP network onto the overlay tracking network containing the special-purpose tracking routers. The attack packets can be easily traced back, hop-by-hop, through the overlay network, from the edge router closest to the victim, back to the entry point of the packet flood into the ISP’s network.

Packet Marking

In packet marking, packets are marked to identify their traffic class. Once the type of traffic is identified, it can be marked, or “colored,” within the packet’s IP header. Packets are colored by marking the IP precedence or the DSCP field to divide them into groups so that end-to-end quality of service (QoS) policies can be applied.

In deterministic packet marking, the router shows all the packets, while in probabilistic packet marking, the path information is divided into small packets.

Probabilistic Packet Marking (PPM)

In packet marking, tracking information is placed into rarely used header fields inside the IP packets themselves. The tracking information is collected and correlated at the destination of the packets, and if there is a sufficiently large packet flow, there will be enough tracking information embedded in the packets to successfully complete the trace.

An attacker can tamper with, or spoof, the tracking information. This method is enhanced by adding authentication to the embedded encodings of tracking information. All of the probabilistic traceback approaches depend on auditing very sparse samples of large packet flows and thus are well suited for attacks that generate massive packet flows, such as DDoS floods. These approaches are not useful for tracking attacks that employ only a small number of packets.

Check Domain Name System (DNS) Logs

The attacker uses DNS to find the actual IP address of the target computer before the attack is introduced. If an attacker uses an attack tool to determine the IP address, then the DNS query closest to the attack could help to identify the attacker’s DNS resolver. It can be useful to compare DNS logs of different systems that are under attack. Using DNS logs, an investigator can identify the different attacks carried out within the same individual or group. Sawmill DNS log analyzer can help view and analyze DNS log files.

Tracing with “log-input”

The following are the steps an investigator should take to trace an attack passing through a router using “log-input”:

1. Make an access list entry that goes with the attack traffic.
2. Attach the log-input keyword to it.
3. Use the access list outbound on the interface through which the attack stream is sent toward the destination.

Log entries produced by the access list discover the router interface from which the traffic arrives and, if the interface is a multipoint connection, provide the layer 2 address of the device from where it is received. Use the layer 2 address to identify the next router in the chain, using show ip arp mac-address.

Control Channel Detection

A large volume of control channel traffic indicates that the actual attacker or coordinator of the attack is close to the detector. The control channel function provides facilities to define, monitor, and control channels. An investigator can use a threshold-based detector to determine the particular number of control channel detectors