1. What is IRC?

IRC stands for "Internet Relay Chat". It was originally written by Jarkko Oikarinen in 1988. Since starting in Finland, it has been used in over 60 countries around the world. IRC is a multi-user chat system, where people meet on "channels" (rooms, virtual places, usually with a certain topic of conversation) to talk in groups, or privately. There is no restriction to the number of people that can participate in a given discussion, or the number of channels that can be formed on IRC.

As a user runs a "client" program which connects to a "server" in an IRC network. All servers are interconnected and pass messages from user to user over the IRC network. One server can be connected to several other servers and up to hundreds of clients.

2. What message is sent by an IRC client when it asks to join an IRC network?

I have compiled Snort with the given binary log file. Afterwards, I viewed those logs with the Analysis Console for Intrusion Databases.

The next step was to find out what is the communication in the log file. The first observation was ‘172.16.134.191’ is our honeypot and the traffic is to and fro from the honeypot. I observed that honeypot is initializing some communication with external servers especially for port ‘6667’,which is used by IRC clients to contact IRC servers. The honeypot used one string to start the communication.

JOIN #x..... x is the message sent by IRC client to join the IRC network.

3. What is a botnet? What are botnets commonly used for?

   In IRC, a botnet consists of one or more bots connected together. This can allow bots to communicate with each other securely, control floods efficiently, and share user lists, ban lists, exempt/invite lists, and ignore lists (if sharing is enabled).

   Botnet is network of compromised hosts, which are used by hackers to have DDOS attacks over other hosts.

4. What TCP ports does IRC generally use?

Internet Relay Chat generally uses any port from 6660 to 6669.

5. What is a binary log file and how is one created?

The binary log file is created when a particular activity is captured by a specific application. We can use this file to view such activities in future. We can configure an application for logging and thus that application creates a log file with our customizable options.

6. What IRC servers did the honeypot, which has the IP address 172.16.134.191, communicate with?

The challenge was to find out the specific characteristics of the IRC servers. IRC servers run on the port between 6000-6009 was the input for searching these hosts. I searched for these ports as the destination ports or service in the ACID and 172.16.134.191 as the source IP. I came to the conclusion that the honeypot has contacted the following IRC servers-

63.241.174.144,

66.33.65.58,

209.126.161.29,

209.196.44.172,

217.199.175.10

7. During the observation period, how many distinct hosts accessed the botnet associated with the server having IP address 209.196.44.172?

Here, the task was to find out the servers, which are communicating with 209.196.44.172. It was clear that 209.196.44.172 was a IRC server. So I had to find out that whether the hosts were trying to access other ports of this server also. ACID gave me the answer for both of these questions. Only 172.16.134.191 accessed 209.196.44.172 and for the IRC service port itself.

8. Assuming that each botnet host has a 56 kbps network link, what is the aggregate bandwidth of the botnet?

Basically, the first question was how to detect any botnet activity. The botnet is famous for DDOS attacks. So, the step was to find out the activities similar to DDOS attacks. After digging out the logs, finally got 11 Ips, which had tried to spread out this, attacks further. So the average bandwidth may be 1MBPS.