I will introduce the DoS attack with UDP flood.

Firstly, let’s take a look at what devices we need to complete this experiment, which are 3 personal computers and a router. It should be emphasized that 3 computers have different roles. One act as an attacker, Kali Linux has been installed on PC1. The second PC is a visitor, it will visit the ftp server to check its working state before and during the UDP flood attack experiment. A FTP server is established on the third computer, providing ftp service and also play the role as a victim.

Before the attack, ping command are sent among all the PCs to ensure that all the devices are connected with each other via the router. This table records the FTP server response time. As you can see on the screen, the maximum is 244 milliseconds, the minimum is 2 milliseconds and the average is 34 milliseconds. Most importantly, there’s no packet loss.

This picture shows the view of the visitor when visiting the FTP server. It can successfully log in and read or write the documents shared by the server.

Then the UDP flood is launched. There are 3 set of experimental data based on different UDP packet size. On the screen, you will obviously find that the average response time increases and the nearly half of the packets are lost.

At that time, if the visitor tries to log on the FTP server, he will find that there is a connection timeout, because the attacker uses UDP flood to block the connection between the visitor and FTP server.

In conclusion, In the experiment of Denial of Service Attack with UDP Flood, the response time of the FTP server is proportional to the packet size, which implies that the attack with lager packet size will be more effective.