1. Screenshots are attached.
2. Before the attack, OWASP Broken Web App displayed a single entry in the ARP table containing “? (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0”. After the attack, the 10.0.2.1 entry is still present and an additional entry appears in the table containing “? (10.0.2.3) at 08:00:27:b2:09:1a [ether] on eth0”. I also noticed that while urlsnarf was running, the ARP entry for (10.0.2.1) was spoofed and appeared as (10.0.2.3).
3. After inspecting the packets in Wireshark, I noticed that the attack begins with packets containing ARP protocol. These packets show that my MAC address is associated with both the victim IP (10.0.2.4) and the router IP (10.0.2.1). When the OWASP Broken Web App (10.0.2.4) is accessing google.com, packets appear containing DNS and TCP protocols. When the request is intercepted and forwarded by my machine, a packet containing the ICMP protocol and “Redirect for host” message appears. Next, a packet containing the HTTP protocol and “166 GET / HTTP 1.0” message is intercepted and forwarded with another ICMP redirect appearing. Finally, TCP packets showing communication between google.com and the victim machine appear, followed by a “HTTP/1.0 200 OK” message and a final ICMP redirect before going back to packets containing ARP protocol.