To begin understanding what was going on in this capture, I first narrowed my search to packets with an IP address (either source or destination) of **192.168.209.10**. This IP address was, according to the project document, assigned to the server on which was hosted the web server, DHCP server, and DNS server. After applying this filter, I found standard DNS, HTTP, and SSH traffic. However, some abnormal-looking traffic stood out from the rest and began to raise my suspicion. From what I see in packets 661 to 664 and from some searching on the protocol these packets were using (BJNP), I believe the attacker began scanning the network, mapping network devices and open ports using NMAP. Starting with simple ARP Packets 1251 to 7248 appear to be a SYN port scan from a device on the network with the IP address **192.168.209.4**. This scan works by sending TCP SYN packets to ports on three different hosts [**192.168.209.1** (management.local), **192.168.209.3** (marketing.local), and **192.168.209.10** (local server)] looking for a SYN-ACK response indicating that the target port is open. Since most of these ports are closed, the majority of the packets sent to the ports receive RST-ACK responses. However, three of the SYN packets sent as part of this port scan received the SYN-ACK response, indicating that those ports were open: port 53 (in packets 1330 and 1331), port 80 (in packets 1391 and 1392), and port 22 (in packets 1401 and 1402) on **192.168.209.10**. These ports are the standard for DNS, HTTP, and SSH, respectively.

Following this port scan, **192.168.209.4** can be seen attempting to connect to the HTTP server located on port 80 of the host server (**192.168.209.10:80**). At first, they attempt to connect without HTTP basic authentication (packet 7267), resulting in a response from the server indicating that they were unauthorized to access it (packet 7269). Then, they begin trying typical username and password combinations such as “admin:admin” (packet 7271), “admin:password” (packet 7274), “admin:1234” (packet 7279), “admin:nimda” (packet 7291), “root:toor” (packet 7301), “password:password” (packet 7306), “admin:passwd” (packet 7318) and “admin:????” (packet 7331).

After being unable to brute force the login for the HTTP server, the attacker cleverly decides to attempt a man-in-the-middle attack, posing as the web server on the network, as evidenced by the duplicate IP addresses (**192.168.209.10**) detected by an ARP request made in packet 7394. When a local marketing client then attempts accesses the web server on **192.168.209.10:80** using HTTP basic authentication with the username “daniel” and password “awesome” (packet 7544), the attacker intercepts these packets and is able to decrypt the authentication, since it only uses base-64 encryption.

The attacker is now able to access the web server using the username and password they intercepted, viewing an “internal_letter.html” document found in packet 7829.