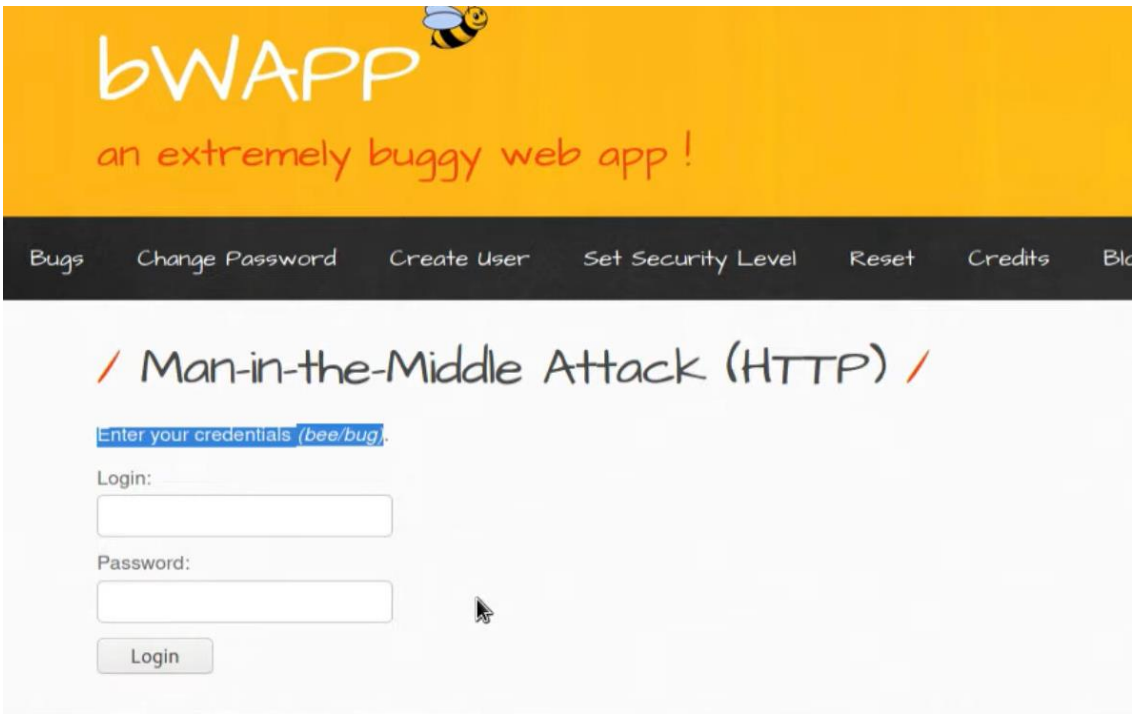
man-in-the-middle attack (http) –

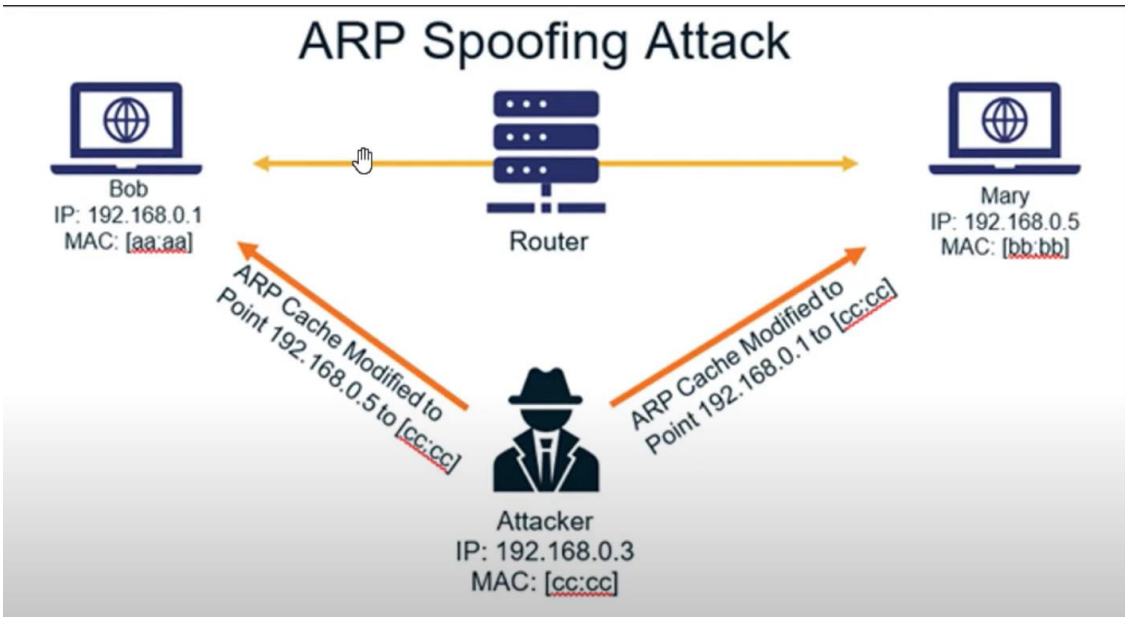
Proof of Concept

Description :

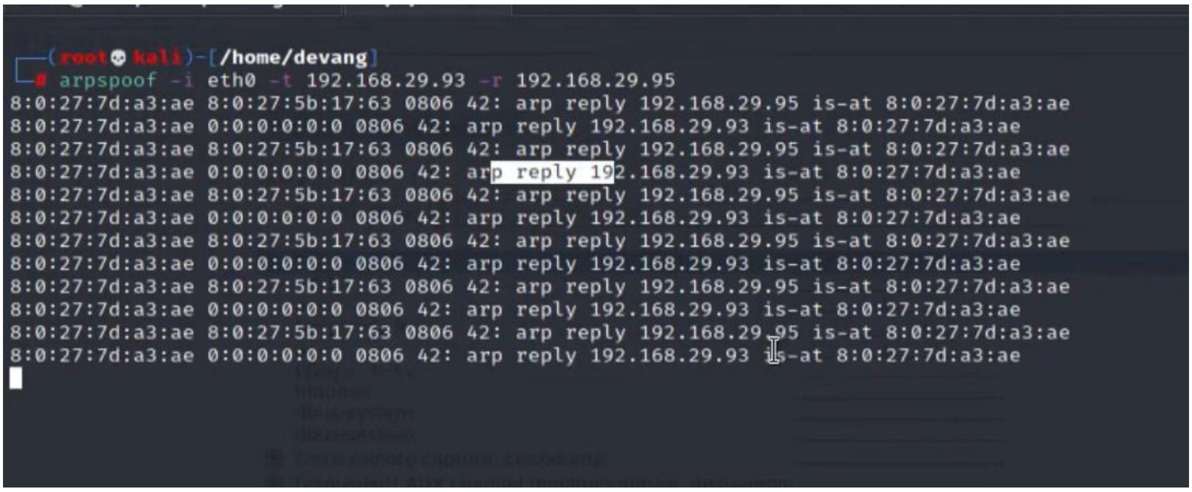
A Man-in-the-Middle (MITM) attack over HTTP occurs when an attacker secretly intercepts and possibly alters communication between a client (such as a browser) and a server. Since HTTP traffic is not encrypted, attackers can read, inject, or modify the data in transit. This can lead to credential theft, session hijacking, or injecting malicious content like scripts or malware. MITM attacks on HTTP are common in open Wi-Fi networks or poorly secured environments, which is why HTTPS (encrypted communication) is strongly recommended to prevent such attacks.



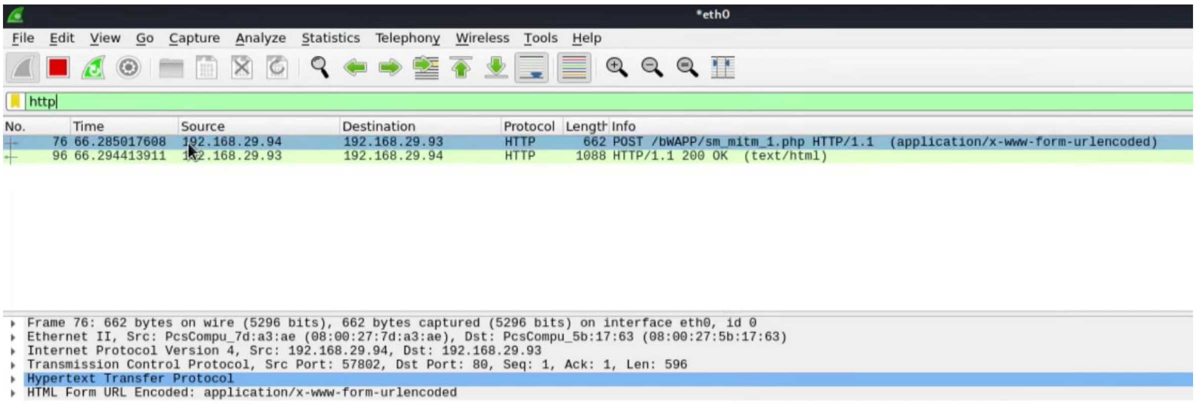
ARP spoofing is when an attacker fakes ARP messages to link their MAC to another IP (usually the gateway), enabling traffic interception or disruption. Prevent with network controls (DAI/DHCP snooping), static ARP, or encryption (VPN/HTTPS).



Start by ARP-Spoofing



Go to wireshark and capture the request after login-in and filter it by http requests



Since the site is not SSL/TLS certified the data it not encrypted and hence is visible

We can see the login credentials that we captured through ARP-Spoofing