DNS cache poisoning based on MITM using ARP spoofing

Yoel Bassin and Dov Greenwald, JCT, November 2020.

Summary

This DNS cache poisoning is based on two main modules, the ARP spoofer and the packet forwarding.

1. ARP spoofing:
   This module actively sends is_at ARP messages every d seconds (2 by default) to fake a connection between the target and the attacker, disguising as the networks Gateway.
2. Packet forwarding:
   This module forwards the messages it gets from the target (after faking the connection) to the real network gateway, except DNS requests for a specified domain. If the attacker (the host) gets an DNS request for the specific domain, it will respond with a fake DNS answer including a fake IP address (usually, an IP address of a malicious server). This will cause a DNS cache poisoning since this is a valid response for the query.

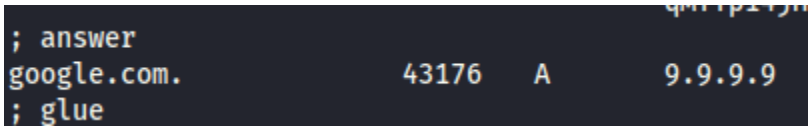

Figure 1 - poisoned cache with google.com represented as 9.9.9.9

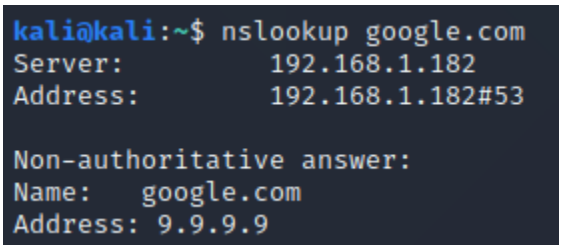

Figure 2 - The DNS poisoning from the user's side (192.168.1.182 is the IP of the DNS server)

This attack will not work in an environment with DNSSEC enabled, because it will not be able to fake an answer with the signature of the real server.

Because the attack does not forward the request to the attacked domain, the attack will fail right away, because it will return to the DNS server a not signed response, which will not be excepted.

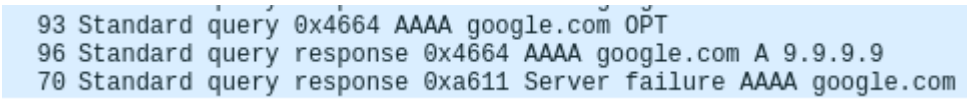

Figure 3 - failure with DNSSEC enabled