**Opened:** Friday, 8 February 2019, 1:30 PM

# Θ-challenge: DHCP spoofing and Man in the Middle

In this challenge, we'll develop different attacks to the Dynamic Host Configuration Protocol (DHCP).

DHCP operation is relatively simple. Once a host connects to the network, it requests an IP address (and the related network configuration) by sending a DHCP DISCOVERY message (in broadcast, identifying the host with its hardware address). That discovery message may be replied by any DHCP server present in the network. Replies are sent back in the form of DHCP OFFER messages, which contain the requested network configuration and the hardware address of the requesting client. The client is expected to accept a proposed configuration (several can be received from several DHCP servers) by sending a REQUEST message to the corresponding DHCP server. As this server acknowledges the requests by sending a DHCP ACK message back, the requested network configuration is granted to the host.

- You can find a more detailed description of DHCP operation e.g. in this tutorial (or some others in the Internet), see RFC 2131 for the technical specification.

**DHCP usurpation**

A first attack consists of usurping the role of a DHCP server, i.e. to interact to the host as a DHCP server -- without being one. As DHCP DISCOVERY message are sent in broadcast, any node connected to the network is in principle able to receive them and fake the behavior of a legitimate DHCP server. If "offered" network configuration is accepted by the host, its Internet connectivity will be compromised.

**DHCP starvation**

DHCP servers maintain a pool of IP addresses that are leased to requesting hosts through the discovery/offer/request process described in the beginning. A classical attack to DHCP, targetting a server pool, is DHCP starvation, i.e. exhausting available IP addresses at a DHCP server by sending too many host requests at a short interval -- so that leasing do not expire before exhaustion of the IP address pool. Note that since requesting hosts identify themselves with their hardware addresses, a malicious host may need to change the requesting HW address to prevent the DHCP server to detect the attack and blacklist the requesting host.

**DHCP spoofing and Man in the Middle**

After starving a legitimate DHCP server, a malicious agent can spoof its identify and manipulate and distribute operational network configurations (and IP addresses) from the spoofed server pool.

In particular, it can provide malicious gateways and DNS servers so that all traffic requested by hosts goes through malicious-controlled nodes. This would allow such malicious agent to become the "Man in the Middle" between the connected host and the Internet -- and thus be in position of eavesdropping Internet traffic or deviating user traffic towards any destination towards a malicious-controlled node of its choice.

- You can find a description of DNS operation and instructions to set up a DNS server (in Debian/Linux) in this tutorial.

As an example, and by combining DHCP starvation, spoofing and gateway/DNS manipulation, as well as by building the corresponding DHCP, DNS and web server, try to achieve that the host receives a page saying "*This is not Facebook*" when requesting for the URL www.facebook.com.

DHCP spoofing

?