Adversary-in-the-Middle: DHCP Spoofing, Sub-technique T1557.003 - Enterprise

Archived: 2026-04-05 17:54:17 UTC

Adversaries may redirect network traffic to adversary-owned systems by spoofing Dynamic Host Configuration Protocol (DHCP) traffic and acting as a malicious DHCP server on the victim network. By achieving the adversary-in-the-middle (AiTM) position, adversaries may collect network communications, including passed credentials, especially those sent over insecure, unencrypted protocols. This may also enable follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation.

DHCP is based on a client-server model and has two functionalities: a protocol for providing network configuration settings from a DHCP server to a client and a mechanism for allocating network addresses to clients.[1] The typical server-client interaction is as follows:

1. The client broadcasts a `DISCOVER` message.
2. The server responds with an `OFFER` message, which includes an available network address.
3. The client broadcasts a `REQUEST` message, which includes the network address offered.
4. The server acknowledges with an `ACK` message and the client receives the network configuration parameters.

Adversaries may spoof as a rogue DHCP server on the victim network, from which legitimate hosts may receive malicious network configurations. For example, malware can act as a DHCP server and provide adversary-owned DNS servers to the victimized computers.[2][3] Through the malicious network configurations, an adversary may achieve the AiTM position, route client traffic through adversary-controlled systems, and collect information from the client network.

DHCPv6 clients can receive network configuration information without being assigned an IP address by sending a `INFORMATION-REQUEST (code 11)` message to the `All_DHCP_Relay_Agents_and_Servers` multicast address.[4] Adversaries may use their rogue DHCP server to respond to this request message with malicious network configurations.

Rather than establishing an AiTM position, adversaries may also abuse DHCP spoofing to perform a DHCP exhaustion attack (i.e, Service Exhaustion Flood) by generating many broadcast DISCOVER messages to exhaust a network's DHCP allocation pool.

Source: https://attack.mitre.org/techniques/T1557/003