SICUREZZA NELLE RETI a. a. 2012/13 – Riassunto DHCP

by Salvatore Fresta

Il **Dynamic Host Configuration Protocol** (DHCP) è un protocollo di rete **locale** il cui compito è quello di fornire **automaticamente** una **configurazione di rete** ai client che ne fanno richiesta. La configurazione è composta da **Indirizzo IP**, **default gateway** e **server DNS**.

Ogni qual volta viene interpellato, il server DHCP sceglie una configurazione di rete dal proprio **pool** (insieme) **di configurazioni**, settato in precedenza dall'amministratore di rete, e la inoltra al client, rendendola, ovviamente, indisponibile per altre richieste, altrimenti si andrebbe incontro a collisioni di indirizzi (non possono esserci in rete due host con lo stesso indirizzo IP). Il numero di configurazioni possibili è **limitato** e viene impostato dall'amministratore.

La richiesta DHCP funziona come segue:

1. Il client che vuole ricevere una configurazione invia in **broadcast** un pacchetto DHCPDISCOVER.
2. Il server DHCP risponde al client con un pacchetto DHCPOFFER.
3. Il client, **se accetta** la configurazione, risponde in **broadcast** (poiché potrebbero esserci altri server DHCP) con un pacchetto DHCPREQUEST.
4. Il server risponde con DHCPPACK.

ATTACCO N. 1

Essendo un protocollo di rete locale, i nodi condividono lo stesso mezzo trasmissivo e sono **identificati dal proprio MAC address**. Un attaccante potrebbe quindi inviare al server DHCP numerose richieste di configurazione con MAC address differenti, **esaurendo** il pool di configurazioni. In questo modo impedisce a **client leggittimi** di ottenere una configurazione di rete.

È possibile limitare questo attacco riservando la configurazione di rete solo per un intervallo di tempo, per poi farla tornare disponibile nel pool. Questa tecnica è nota come **leasing**.

Alcuni switch inoltre permettono di avere per ogni borchia un numero limitato di MAC address.

ATTACCO N. 2

Un attaccante potrebbe allestire un **rougue DHCP server** all'interno della rete. Ovviamente le risposte di questo server DHCP malevolo devono arrivare al client **prima** di quelle del server legittimo.

In questo modo è possibile:

- **sostituirsi al default gateway** ed intercettare tutto il traffico senza porre la scheda in modalità promiscua, in quanto il client compromesso invierà coscientemente il traffico alla macchina attaccante.

- **sostituirsi al server DNS** e manipolare la risoluzione dei nomi a dominio.

Per impedire che ciò avvenga, l'amministratore dovrebbe monitorare la rete e forzare l'uso di server DHCP solo in una determinata borchia, o adottare estensioni di DHCP con autenticazione.