Dissector per traffico MDNS

Luca Montemaggi

12 giugno 2018

`Dmdns` è un dissector MDNS che ricerca e stampa richieste e risposte MDNS.

1 Introduzione

1.1 Il protocollo MDNS

MDNS (Multicast DNS) è un protocollo definito in RFC6762, utilizzato per risolvere *hostname* in IP entro un piccolo network che non include un name server locale.

MDNS è un servizio *zero-configuration* che utilizza le stesse interfacce e formato dei pacchetti di *unicast DNS*, creato per essere capace di operare in modo *standalone*.

MDNS utilizza il protocollo UDP sulla porta `5353`, usando gli indirizzi `224.0.0.251` per IPv4 e `FF02::FB` per IPv6.

1.2 Progetto

Il progetto si pone lo scopo di intercettare sull'interfaccia stabilita tutti i pacchetti MDNS e di analizzare il payload per stampare le *query* o i *response* dei device MDNS presenti.

1.3 Come utilizzare il progetto

Per la realizzazione del progetto viene utilizzata la libreria nDPI (versione 1.8-stable).Per utilizzarla é necessario fare git clone del progetto, entrare nella cartella e compilare ed installare con ./configure && make && make install.

Per compilare il progetto si entra nella cartella e si esegue il comando make, il file eseguibile risultante `Dmdns` si esegue con ./Dmdns -i <device>, il device da cui eseguire lo scan.

2 Realizzazione

Il progetto va a modificare il plugin `mdns.c` del progetto nDPI, per migliorare la gestione dei pacchetti MDNS per le richieste e le risposte, per stampare il nome del modello, il tipo di device e il nome, ed inserire il nome nella struttura `flow->host_server_name`.

Per testare il plugin si realizza del codice per vedere il funzionamento del plugin, utilizzando la libreria `libpcap` per la cattura dei pacchetti e la libreria `ndpi` per analizzare il contenuto del pacchetto catturato.

Il file `collecmdns.c` registra una callback `onfindmdns` che viene richiamata ogni volta che viene trovato un pacchetto MDNS, dopo aver settato la maschera `NDPI_PROTOCOL_MDNS`. Questo è svolto utilizzando le funzioni fornite dalla libreria `ndpi_util.h` ed implementate in `ndpi_util.c`.

Al progetto viene passata per argomento (`-i <device>`) l'interfaccia tramite cui fare lo scan della rete. Una volta ricevuto il pacchetto: se corrisponde a un pacchetto MDNS viene chiamata la funzione `onfindmdns` che esegue la funzione che controlla se è un pacchetto MDNS, ma dato che se viene chiamata la funzione significa che il protocollo è stato trovato. Se non lo è, di conseguenza, viene scartato. La modifica al plugin `mdns.c` con la funzione `FlowdissectMDNS` permette di risolvere i nomi e quindi i servizi offerti di chi utilizza in quella rete locale il protocollo MDNS.