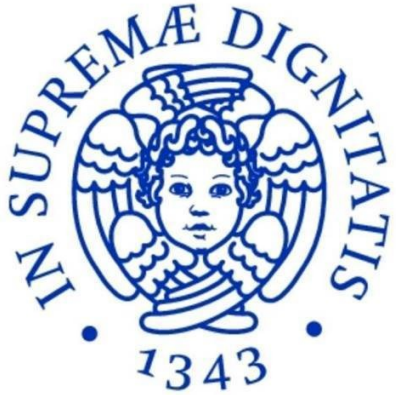

Università degli Studi di Pisa

Progetto Gestione di Rete

Titolo: Estensione nDPI
Studente: Alessandro Bondielli
Matricola: 503777
Anno: 2018-19

1. INTRODUZIONE

nDPI è una libreria open source, scritta in C, utilizzata per effettuare Deep Packet Inspection. E' stato modificato il file nDPIReader.c per fare in modo che ci sia la possibilità di stampare, in un file, la lista univoca dei DHCP - Fingerprint.

2. FUNZIONAMENTO

L'eseguibile di nDPIReader, contenuto nella sottocartella example di nDPI, permette con l'opzione -i che gli venga passato un parametro (un file) da cui leggere dati; questo file è di tipo pcap, ossia è una cattura di wireshark di un insieme di pacchetti, da cui nDPI riesce a estrapolare il DHCP – Fingerprint di ogni pacchetto e stamparlo a video.
La modifica consiste nell'aggiungere un flag per implementare la funzionalità di poter stampare la lista univoca dei DHCP in un file, il cui nome è passato come parametro all'eseguibile.

3. IMPLEMENTAZIONE

E' stata aggiunta una variabile globale per contenere il nome del file da creare (e aprire) e su cui scrivere i DHCP - Fingerprint.
Per poter richiedere la stampa in un file bisogna lanciare l'eseguibile con l'opzione -k <file> dove <file> indica il nome del file ed è obbligatorio che sia presente (si potrebbe rendere opzionale la presenza del nome -modificando la riga 337 del codice- e nel caso non sia specificato, creare un file nuovo con un nome 'predefinito' es. fingerprint_list.txt).
Quando viene lanciato l'eseguibile viene fatto il parse delle varie opzioni e viene controllato se è presente -k; nel caso ci sia creo il file col nome associato, ritornando un errore se è gia presente un file con quel nome (questa è una scelta personale perchè non volevo nè cancellare il vecchio contenuto del file nè aggiungere dati alla fine del file, però è possibile cambiarlo -modificando la riga 643 del codice- e gestirlo come si vuole).
Prima di scrivere un nuovo DHCP - Fingerprint nel file, questo viene confrontato (scorrendo il file riga per riga) con i DHCP già presenti, per evitare di scrivere due o più volte lo stesso fingerprint; questo perché un host, dentro una cattura, potrebbe avere più pacchetti dhcp associati e si vuole evitare di ripetere lo stesso fingerprint

nella lista.
Alla terminazione del programma, il file se era stato aperto viene chiuso.
Un problema è che se non è presente l'opzione -verbose 2, la stampa dei DHCP non avviene, questo perchè non vengono letti tutti i pacchetti e calcolati i relativi DHCP; una possibile soluzione sarebbe quella di 'forzare' l'opzione -v 2 quando è presente -k (togliendo il commento '//' alla riga 650), però questo risolve parzialmente il problema perchè se per esempio il programma viene lanciato con -v 1 dopo -k <file> (es. ./ndpireader -i dhcp.pacp -k fingerprint_list.txt -v 1), in questo caso il -v 1 sovrascrive la 'forzatura' di k e non viene stampato nulla nel file.
Ovviamente, omettendo il -k, è sempre possibile stampare a video senza stampare nel file.

4. TESTING

Prima di testare il file, bisogna compilare la libreria nDPI nel seguente modo:
- ./autogen.sh
- ./configure
- make
I prerequisiti per la compilazione comprendono: GNU tools(autogenm, automake, autoconf, libtool) e GNU C compiler (gcc).

Per testare la funzionalità aggiunta bisogna spostarsi nella sottocartella example di nDPI e lanciare da terminale il comando './ndpireader -i dhcp.pcap -v 2 -k fingerprint_list.txt'. Serve un file da passare come parametro -i da dove leggere tutti i pacchetti DHCP, precedentemente sniffati, di cui si vuole avere il fingerprint (il file .pcap deve trovarsi dentro la cartella nDPI non in example e, analogamente, il file desiderato viene creato li). E' stato testato su un pc con sistema operativo MacOS Sierra ed anche sulla macchina virtuale con una versione di linux (Ubuntu), però entrambe solo con un file .pcap (potrei fare uno script per provarlo sequenzialmente su più file .pcap).

5. ESEMPIO

Di seguito due foto che espongono un esempio di test; la prima immagine mostra il risultato ottenuto dall'esecuzione di ndpiReader e la seconda indica la cattura dei pacchetti usata.

```
List of DHCP - Fingerprint:
1,3,6
1,28,2,3,15,6,119,12,44,47,26,121,42,249,33,252
1,28,2,3,15,6,119,12,44,47,26,121,42,121,249,33
```

Lista univoca dei DHCP – Fingerprint.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	294	DHCP Discover - Transaction ID 0x6c280fff
2	60.021071	0.0.0.0	255.255.255.255	DHCP	294	DHCP Discover - Transaction ID 0x55b20fff
3	120.031851	0.0.0.0	255.255.255.255	DHCP	294	DHCP Discover - Transaction ID 0xb140fff
4	138.522152	192.12.193.41	192.12.193.124	DHCP	342	DHCP Request - Transaction ID 0xc4907d6f
5	180.047976	0.0.0.0	255.255.255.255	DHCP	294	DHCP Discover - Transaction ID 0x58be0fff
6	240.063902	0.0.0.0	255.255.255.255	DHCP	294	DHCP Discover - Transaction ID 0x31eb0fff
7	300.075964	0.0.0.0	255.255.255.255	DHCP	294	DHCP Discover - Transaction ID 0x3510fff
8	309.041083	192.12.193.86	192.12.193.124	DHCP	342	DHCP Request - Transaction ID 0x93672768
9	337.801064	0.0.0.0	255.255.255.255	DHCP	590	DHCP Request - Transaction ID 0x369c0f69
10	360.087984	0.0.0.0	255.255.255.255	DHCP	294	DHCP Discover - Transaction ID 0x3d00fff
11	408.276260	192.12.193.11	192.12.193.124	DHCP	342	DHCP Request - Transaction ID 0xe8988717
12	408.279341	192.12.193.124	192.12.193.11	DHCP	342	DHCP ACK - Transaction ID 0xe8988717
13	420.103874	0.0.0.0	255.255.255.255	DHCP	294	DHCP Discover - Transaction ID 0x65e00fff

File di cattura pacchetti di Wireshark con filtro DHCP.