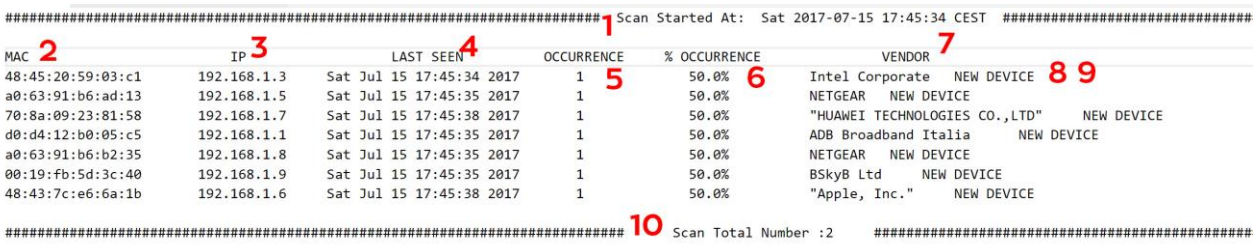
hARPer- A local network logger

hARPer è un software multithread basato sulla libreria **pcap**, il quale sfrutta il protocollo ARP per effettuare scansioni periodiche della rete locale. HARPer tiene traccia dei dispositivi connessi alla rete salvando le loro informazioni su un file di log,
segnalando i dispositivi sconosciuti alla rete e gli eventuali IP duplicati rilevati all'interno della scansione stessa.

Come funziona?

hARPer è composto da tre thread: il main, un injector e un receiver.

- **L'injector** si occupa di forgiare un pacchetto ARP per ogni IP appartenente alla sottorete, la quale viene ricavata dall'IP dell'interfaccia del PC sul quale è in esecuzione e dalla subnet mask. Infine invia questi pacchetti in broadcast, per un numero di volte definito dall'utente (di default 2) a intervalli regolari (di default 20ms) di durata personalizzabile. È importante notare che avere intervalli troppo piccoli implica l'aumento della probabilità che il receiver perda pacchetti, mentre mandare troppe volte lo stesso pacchetto genera traffico inutile. L'interfaccia di rete utilizzata è ricavata automaticamente. Può comunque essere specificata con l'opzione -i.
- **Il receiver** si occupa di catturare pacchetti filtrando le risposte ARP, quindi di processarli leggendo il MAC e l'IP del sender e inserirli in una hash table. Per ogni MAC vengono mantenuti in memoria l'ultimo IP assegnatogli e il timestamp della sua ultima apparizione.
- **Il main** si occupa di mantenere persistenti le informazioni codificate all'interno della hashtable utilizzando un file *dump_ht.csv*. L'hashtable viene creata e distrutta rispettivamente ad ogni avvio e termine di una istanza di hARPer. *dump_ht.csv* tiene traccia di tutti i device apparsi fin dal primo avvio del programma. Il main si occupa anche della funzione principale di hARPer. Ovvero quella di aggiungere a un file *log.txt* le seguenti informazioni relative all'ultima scansione:



1. Data e orario della scansione.
2. MAC dispositivo connesso.
3. IP associato al MAC.
4. Timestamp del momento della rilevazione.
5. Numero di apparizioni dal primo lancio del programma.
6. Percentuale del numero di apparizioni rispetto al numero di numero di esecuzioni del programma.
7. Nome del vendor della scheda di rete.
8. FLAG prima apparizione.
9. FLAG MAC duplicati.
10. Contatore del totale numero di scansioni.

Requisiti

- CMAKE
- A GCC compiler
- Libreria libpcap-dev

Come mandare hARPer in esecuzione?

Dopo aver compilato il programma, per lanciarne una singola istanza è sufficiente eseguire *harper* con i privilegi di root.
Per eseguire periodicamente hARPer in background, abbiamo scritto un script bash *harper_installer.sh* il quale sfrutta il demone *cron,* impostando una crontab*.*
Sia *harper* che *harper_installer.sh* possono essere lanciati con delle opzioni:

sudo ./harper [-i <interface>] [-r <repetitions>] [-t <intervals>]

-i interface = nome dell'interfaccia di rete utilizzata

-r repetitions = numero di richieste ARP inviate per ogni singolo IP appartenente alla sottorete.

-t intervals = tempo in millis che intercorre tra l'invio di due richiete ARP

sudo bash harper_installer.sh [-i <interface>] [-r <repetitions>] [-f <output_file>] [-t <time_between_executions>]

-i interface = nome dell'interfaccia di rete utilizzata

-r repetitions = numero di richieste ARP inviate per ogni singolo IP appartenente alla sottorete.

-f output_file = file sul quale verrà stampato l'output di harper

-t time = tempo in minuti che intercorre tra due esecuzioni di harper