Rilevamento di mass scan e interruzione della connessione

Andrea Tommasi
a.tommasi7@studenti.unipi.it

Lo scopo del progetto era quello di inserire una porzione di codice che implementasse all'interno del programma "ipt_geofence" dei controlli per rilevare scansioni di massa e bloccare gli host responsabili della scansione.

Per farlo ho inserito, all'interno del file "NwInterface.cpp", un controllo sul tipo di protocollo utilizzato per spedire il pacchetto, poiché la maggior parte dei tool usati per eseguire mass scans utilizzano protocolli "nulli" (nel caso di ipv4 il codice protocollo è 0, nel caso di ipv6 invece è 59).
La porzione di codice aggiunta controlla infatti la variabile "proto" all'interno della sezione di analisi pacchetto ipv6 e ipv4: nel caso in cui la variabile fosse uguale a IPPROTO_IP (che corrisponde al valore 0) per ipv4, o uguale a IPPROTO_NONE (che corrisponde al valore 59) per ipv6, vengono chiamate le funzioni necessarie per notificare la presenza dell'attacco e bloccare la connessione.

Le funzioni utilizzati sono le seguenti:

- *logFlow(...)* : funzione utilizzata per notificare la macchina della presenza di un pacchetto appartenente ad una mass scan, comunicando anche l'ip sorgente, la porta sorgente, l'ip di destinazione e il luogo da cui è stato spedito.
- *ban(...)* : funzione utilizzata per bandire l'indirizzo ip e il traffico dell'host che stava eseguendo la scansione
- *getMarkerDrop()* : funzione utilizzata per "droppare" il pacchetto rilevato dannoso

Basterà quindi eseguire il programma su una macchina che si trova all'interno della rete da monitorare ed essa inizierà ad analizzare i pacchetti: nel caso in cui ne trovasse uno appartenente ad una mass scan, lo rimuove dalla coda e blocca le connessioni dell'host mittente.