Relazione sul progetto di Gestione di Rete

Mario Coco e Federico Finocchio

Introduzione

HOKER è un tool per il monitoraggio degli host connessi ad una rete locale basato sulla libreria pcap che sfrutta il protocollo ARP per immagazzinare informazioni come:

- Associazioni MAC-IP
- Connessioni e disconnessioni dalla rete

Struttura HOKER

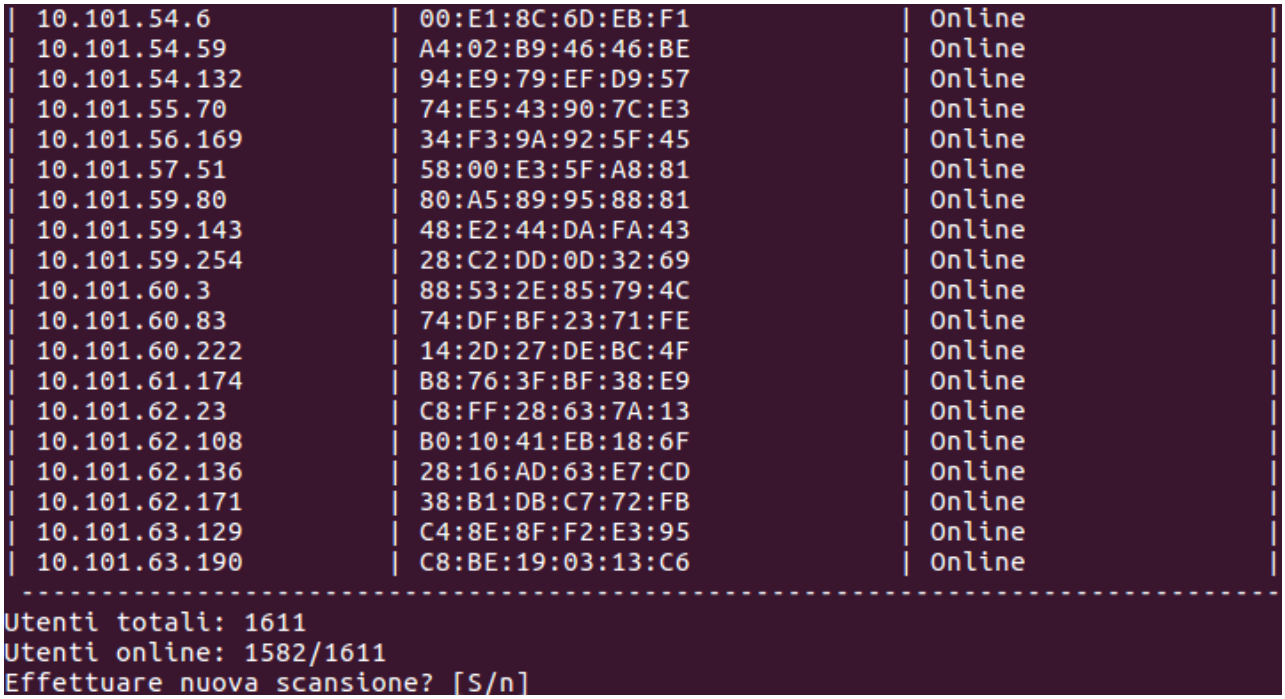
HOKER ha una struttura multi-threaded della quale si riportano i principali thread in gioco:

- **Discoverer**: crea un frame ethernet contenente una richiesta ARP e lo inoltra a tutti gli utenti connessi alla rete locale, ciclando su tutti gli indirizzi IP del blocco. Il tempo di attesa tra l'invio di una richiesta ARP e l'altra è di 2 millisecondi.
- **Sniffer**: filtrando i soli pacchetti ARP di risposta destinati all'host su cui è in esecuzione HOKER, salva le informazioni relative agli host (MAC, IP, stato) in una hash map (https://github.com/rxi/map).

Il **main** si occupa: delle operazioni legate all'inizializzazione dell'interfaccia di rete, della compilazione e del settaggio del filtro per i pacchetti ARP, del reperimento della maschera di rete e del blocco di indirizzi IP, della creazione dei due thread prima menzionati.

Riordina infine le informazioni ricavate dall'operazione di scansione, stampandone i risultati e proponendo all'utente la possibilità di effettuare una nuova scansione. Le scansioni successive determineranno lo stato in rete degli host già scansionati.

Esempio di utilizzo



Note

Il tool funziona correttamente su Ubuntu 16.04 LTS.