

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

```
| 10.101.54.6 | 00:E1:8C:6D:EB:F1 | Online |
| 10.101.54.59 | A4:02:B9:46:46:BE | Online |
| 10.101.54.132 | 94:E9:79:EF:D9:57 | Online |
| 10.101.55.70 | 74:E5:43:90:7C:E3 | Online |
| 10.101.56.169 | 34:F3:9A:92:5F:45 | Online |
| 10.101.57.51 | 58:00:E3:5F:A8:81 | Online |
| 10.101.59.80 | 80:A5:89:95:88:81 | Online |
| 10.101.59.143 | 48:E2:44:DA:FA:43 | Online |
| 10.101.59.254 | 28:C2:DD:0D:32:69 | Online |
| 10.101.60.3 | 88:53:2E:85:79:4C | Online |
| 10.101.60.83 | 74:DF:BF:23:71:FE | Online |
| 10.101.60.222 | 14:2D:27:DE:BC:4F | Online |
| 10.101.61.174 | B8:76:3F:BF:38:E9 | Online |
| 10.101.62.23 | C8:FF:28:63:7A:13 | Online |
| 10.101.62.108 | B0:10:41:EB:18:6F | Online |
| 10.101.62.136 | 28:16:AD:63:E7:CD | Online |
| 10.101.62.171 | 38:B1:DB:C7:72:FB | Online |
| 10.101.63.129 | C4:8E:8F:F2:E3:95 | Online |
| 10.101.63.190 | C8:BE:19:03:13:C6 | Online |
-----
Utenti totali: 1611
Utenti online: 1582/1611
Effettuare nuova scansione? [S/n]
```

Note

Il tool funziona correttamente su Ubuntu 16.04 LTS.