

執行環境與操作：

- a. OS: UBUNTU 13.10
- b. compile: gcc -o arp arp_reply_attack.c
- c. run: ./arp
- d. 有小 bug，必須在 tcpdump 監聽下才會抓到正確的被攻擊者 MAC address，直接執行 arp 會抓錯。

程式解釋：

- a. 程式裡面所使用的函式與自己比較不清楚的函式使用：
 - 1. char *allocate_strmem (int len); 為分配記憶體空間給 char 型態的陣列空間。
 - 2. uint8_t * allocate_ustrmem (int len); 為分配記憶體空間給 unsigned char 型態的陣列空間。
 - 3. inet_pton(int af, const char *src, void *dst): 將 src 字串轉成網路位址 af 的 address family 結構，並將結果複製到 dst 字串，且 af 參數需為 AF_INET 或者 AF_INET6，回傳值部份為 1 是成功轉換，0 為 src 字串非正確的 address family 結構，-1 則是 af 為不正確的 address family。
- b. 變數說明：
 - 1. int sd: socket descriptor。
 - 2. char* interface: 網路的介面名字。
 - 3. char* target: 接收端的 ip 或者 URL，必須在 LAN 內(link-local node)。
 - 4. char* src_ip: 傳送端的 ip。
 - 5. uint8_t *dst_mac: 接收端的 MAC 位址。
 - 6. uint8_t *src_mac: 傳送端的 MAC 位址。

7. uint8_t *ether_frame: ethernet 的框架，框架結構為 ethernet header(接收端的

MAC(6)+傳送端的 MAC(6)+ethernet type(2)) 加上 ethernet data(ARP 標頭(28)), 括號數字內為 byte 數。

8. struct sockaddr_in *ipv4: IPv4 的 socket 位址結構。

c. 程式概述：

此程式的被攻擊者為 **140.116.96.121**，其 MAC address 為 **00:24:8c:d9:c9:01**。

Main function 開始，一開始先分配記憶體給各個所需陣列，接著原本的程式是利用 socket 得到傳送端的 MAC 位址及網路介面並輸出，這邊可以將其改成任意的 MAC 位址來騙人。

之後輸出 interface 的 index，藉由 if_nametoindex(介面名子)的方式。

之後流程為設定傳送端 MAC 位址為 FF: FF: FF: FF: FF: FF(即 broadcast)的 ARP

request，以取得被攻擊者的 MAC address(藉由察看 arp header 的第 22 個數字是否為 2，2

即是被攻擊者的 ARP REPLY，來確認是否封包為被攻擊者的)，之後就可以從 arp header

裏面得到被攻擊者的 MAC address 了。最後再用 ARP REPLY 的方式告知被攻擊者說

gateway 的 MAC ADDRESS 是 12:34:56:78:9A:BC 也就是假的 MAC address，以達到攻擊的目的。

```
Guake Terminal
18:14:28.079775 e8:39:35:3d:24:70 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.219 tell 140.116.96.220, length 46
18:14:28.349447 00:1d:aa:83:54:d0 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.4 tell 140.116.96.253, length 46
18:14:28.387443 00:1d:aa:83:54:d0 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.4 tell 140.116.96.253, length 46
18:14:28.833590 f4:6d:04:f0:d5:30 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.109 tell 140.116.96.171, length 46
18:14:28.852193 00:1d:aa:83:54:d0 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.253 tell 140.116.96.150, length 46
18:14:28.852206 00:1d:aa:83:54:d0 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.253 tell 140.116.96.157, length 46
18:14:29.083331 14:da:e9:96:ae:0b (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.225 tell 140.116.96.210, length 46
18:14:29.079879 e8:39:35:3d:24:70 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.219 tell 140.116.96.220, length 46
18:14:29.252258 12:34:56:78:9a:bc (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 42: Reply 140.116.96.253 is-at 12:34:56:78:9a:bc (oui Unknown), length 28
18:14:29.350374 00:1d:aa:83:54:d0 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.109 tell 140.116.96.197, length 46
18:14:29.578813 12:34:56:78:9a:bc (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 42: Request who-has 140.116.96.121 tell 140.116.96.253, length 46
18:14:29.578995 00:24:8c:d9:c9:01 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Reply 140.116.96.121 is-at 00:24:8c:d9:c9:01 (oui Unknown), length 46
18:14:29.578739 12:34:56:78:9a:bc (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 42: Reply 140.116.96.253 is-at 12:34:56:78:9a:bc (oui Unknown), length 28
18:14:29.579121 00:24:98:11:bf:42 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Reply 140.116.96.253 is-at 00:24:98:11:bf:42 (oui Unknown), length 46
18:14:29.695704 00:24:98:11:bf:42 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.133 tell 140.116.96.253, length 46
18:14:29.721268 00:24:98:11:bf:42 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Reply 140.116.96.253 is-at 00:24:98:11:bf:42 (oui Unknown), length 46
18:14:29.823164 14:da:e9:96:ae:0b (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.225 tell 140.116.96.210, length 46
18:14:30.127448 78:54:2e:e0:5c:c9 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.177 tell 140.116.96.63, length 46
18:14:30.251370 00:1d:aa:83:54:d0 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.109 tell 140.116.96.197, length 46
18:14:30.378919 12:34:56:78:9a:bc (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 42: Reply 140.116.96.253 is-at 12:34:56:78:9a:bc (oui Unknown), length 28
18:14:30.551495 14:da:e9:96:ae:0b (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.225 tell 140.116.96.210, length 46
18:14:31.099850 f0:92:1c:df:27:80 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.219 tell 140.116.96.221, length 46
18:14:31.252437 12:34:56:78:9a:bc (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 42: Reply 140.116.96.253 is-at 12:34:56:78:9a:bc (oui Unknown), length 28
18:14:31.579730 78:54:2e:e0:5c:c9 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.177 tell 140.116.96.63, length 46
18:14:31.579084 12:34:56:78:9a:bc (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 42: Reply 140.116.96.253 is-at 12:34:56:78:9a:bc (oui Unknown), length 28
18:14:31.763330 00:24:98:11:bf:42 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Reply 140.116.96.253 is-at 00:24:98:11:bf:42 (oui Unknown), length 46
18:14:31.822907 f0:92:1c:df:27:80 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.219 tell 140.116.96.231, length 46
18:14:32.579198 17:14:56:78:9a:bc (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 42: Reply 140.116.96.253 is-at 12:34:56:78:9a:bc (oui Unknown), length 28
18:14:32.822895 f0:92:1c:df:27:80 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.219 tell 140.116.96.231, length 46
18:14:32.889253 00:24:98:11:bf:42 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.225 tell 140.116.96.253, length 46
18:14:32.978634 00:9b:c9:f1:d7:9d (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.113 tell 140.116.96.114, length 46
18:14:32.991275 48:5b:39:f9:c6:dc (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.145 tell 140.116.96.156, length 46
18:14:33.252096 12:34:56:78:9a:bc (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 42: Reply 140.116.96.253 is-at 12:34:56:78:9a:bc (oui Unknown), length 28
18:14:33.253995 00:24:98:11:bf:42 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Reply 140.116.96.253 is-at 00:24:98:11:bf:42 (oui Unknown), length 46
18:14:33.724949 00:24:98:11:bf:42 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.44 tell 140.116.96.253, length 46
18:14:33.869294 00:24:98:11:bf:42 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.133 tell 140.116.96.253, length 46
18:14:33.912763 2c:27:d7:12:83:08 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.149 (65:01:02:01:04:01 (oui Unknown)) tell 140.116.96.138, length 46
18:14:33.938444 54:0a:e9:11:c8:b1 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.4 tell 140.116.96.209, length 46
18:14:33.985016 14:da:e9:96:ae:0b (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has name:ncr.edu.tw tell 140.116.96.210, length 46
18:14:33.988975 14:da:e9:96:ae:0b (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has edge-star.shv-04-hk01.facebook.com tell 140.116.96.210, length 46
18:14:33.991248 48:5b:39:f9:c6:dc (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.145 tell 140.116.96.156, length 46
18:14:34.186668 00:25:b3:fc:a4:6c (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.149 (65:6c:6f:70:65:3e (oui Unknown)) tell 140.116.96.26, length 46
18:14:34.502133 54:0a:e9:11:c8:b1 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.4 tell 140.116.96.209, length 46
18:14:34.501255 48:5b:39:f9:c6:dc (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.145 tell 140.116.96.156, length 46
18:14:35.132880 00:23:7d:6f:c1:b0 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.149 tell 140.116.96.55, length 46
18:14:35.163287 14:da:e9:11:c8:b1 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Request who-has 140.116.96.109 tell 140.116.96.204, length 46
18:14:35.252791 12:34:56:78:9a:bc (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 42: Reply 140.116.96.253 is-at 12:34:56:78:9a:bc (oui Unknown), length 28
18:14:35.253383 00:24:98:11:bf:42 (oui Unknown) > Broadcast, ethertype ARP (0x8806), length 60: Reply 140.116.96.253 is-at 00:24:98:11:bf:42 (oui Unknown), length 46
79 packets captured
79 packets received by filter
0 packets dropped by kernel
ping@ping -
vim arp_reply_attack.c ping@ping:~/Desktop ping@ping:~
```

附圖反白部份為最後 ARP REPLY 的部份，反白部份文字如下。

18:14:31.579084 12:34:56:78:9a:bc (oui Unknown) > 00:24:8c:d9:c9:01 (oui Unknown),

ethertype ARP (0x0806), length 42: Reply **140.116.96.253 is-at 12:34:56:78:9a:bc** (oui
Unknown), length 28