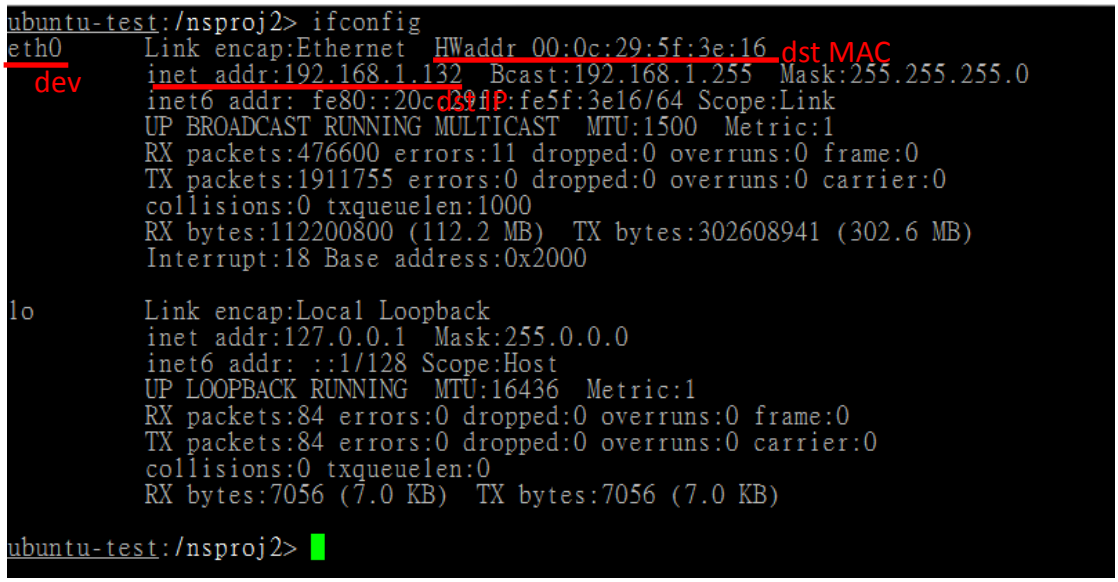
網路安全

Project 2 Report

9617145 資工 3C 許晏峻

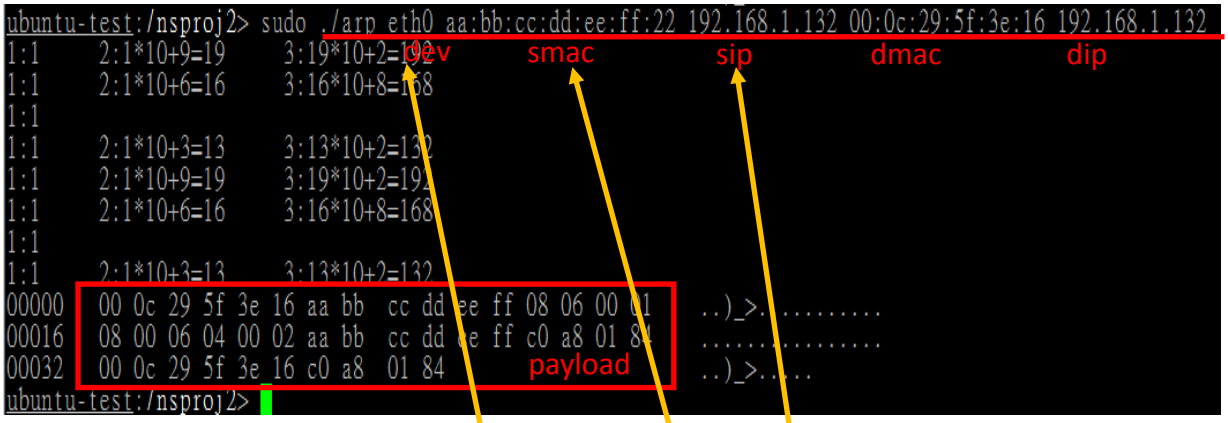
1. 執行截圖：



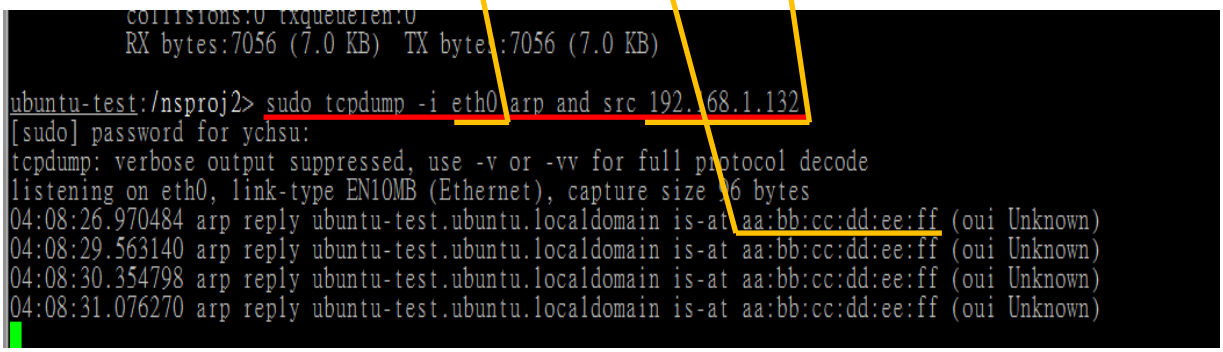

```
ubuntu-test:/nsproj2> ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:5f:3e:16
          inet addr:192.168.1.132  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe5f:3e16/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:476600 errors:11 dropped:0 overruns:0 frame:0
          TX packets:1911755 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:112200800 (112.2 MB)  TX bytes:302608941 (302.6 MB)
          Interrupt:18 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:84 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7056 (7.0 KB)  TX bytes:7056 (7.0 KB)

ubuntu-test:/nsproj2>
```




```
ubuntu-test:/nsproj2> sudo ./arp eth0 aa:bb:cc:dd:ee:ff:22 192.168.1.132 00:0c:29:5f:3e:16 192.168.1.132
1:1     2:1*10+9=19     3:19*10+2=192
1:1     2:1*10+6=16     3:16*10+8=168
1:1
1:1     2:1*10+3=13     3:13*10+2=132
1:1     2:1*10+9=19     3:19*10+2=192
1:1     2:1*10+6=16     3:16*10+8=168
1:1
1:1     2:1*10+3=13     3:13*10+2=132
00000   00 0c 29 5f 3e 16 aa bb  cc dd ee ff 08 06 00 01   ..)_>. ........
00016   08 00 06 04 00 02 aa bb  cc dd ee ff c0 a8 01 84   ........ ........
00032   00 0c 29 5f 3e 16 c0 a8  01 84                     ..)_>. ....
ubuntu-test:/nsproj2>
```



```
          RX bytes:7056 (7.0 KB)  TX bytes:7056 (7.0 KB)

ubuntu-test:/nsproj2> sudo tcpdump -i eth0 arp and src 192.168.1.132
[sudo] password for ychsu:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
04:08:26.970484 arp reply ubuntu-test.ubuntu.localdomain is-at aa:bb:cc:dd:ee:ff (oui Unknown)
04:08:29.563140 arp reply ubuntu-test.ubuntu.localdomain is-at aa:bb:cc:dd:ee:ff (oui Unknown)
04:08:30.354798 arp reply ubuntu-test.ubuntu.localdomain is-at aa:bb:cc:dd:ee:ff (oui Unknown)
04:08:31.076270 arp reply ubuntu-test.ubuntu.localdomain is-at aa:bb:cc:dd:ee:ff (oui Unknown)
```

2. **程式說明：**

基本上完成了 resolve、translate_mac 和 build 三個 function：
resolve 和 translate_mac 做的事很類似，一個(resolve)是把 IP address 轉成 network 可以讀的 order format，另一個(translate_mac)則是把 MAC address 轉成一樣格式的 data，只差在 size 不一樣。而做法就用最笨的方法去判斷字串值一個一個比較存成 hex int 值在存到 char，轉成 1byte data。

而 build 就是將 input 的 5 個參數丟進 ethernet&arp headet 中，放進去後存到一個 char*中，再準備利用 raw socket 將這個 packet 丟出去。

最後建立 raw socket 的地方，先將 dev 丟進 struct sockaddr 中，再來呼叫 socket system call 第二個參數要放 SOCK_PACKET，第三個就要放 ARP protocol。
建好 socket 就用 sendto 將做好的這個 packet 丟出去就 ok 了！

3. **ARP spoofing 防治方法：**
   1. 依靠較安全的 switch：NBADswitch、 NBADsensor、VLAN switch
   2. 防火牆
   3. NIPS 系統
   4. Anti-ARP spoofing

4. **參考資料：**

   1. http://en.wikipedia.org/wiki/Address_Resolution_Protocol
   2. http://www.ipv6.com/articles/general/Address-Resolution-Protocol.htm
   3. http://www.study-area.org/network/network_ip_arp.htm
   4. http://www.tcpdump.org/pcap3_man.html
   5. http://www.enderunix.org/docs/en/rawipspoof/
   6. http://mixter.void.ru/rawip.html
   7. Project2 教學文件
   8. http://en.wikipedia.org/wiki/ARP_spoofing
   9. http://datenterrorist.wordpress.com/2007/07/06/arp-spoofing/
   10. http://amos0601.pixnet.net/blog/post/21975287
   11. http://mmdays.com/2008/11/10/mitm/