ARP 模糊測試攻擊

系所／資訊工程學系
指導老師／徐武孝
組員／林亭均、林微庭、吳柏誼、許琬晴

在當今社會中，網路已成為了普羅大眾日常的一部分，並且在可預見的未來中，網際網路只會越來越貼近人們的生活，工業私企、醫療建設都將繞不開網路，層層纏繞直至密不可分為止。在以此為前提的情況下，對於資訊安全的需求自然不可同日而語，若仍停留在從前，可能造成的危害不堪設想。

隨著資訊科技的進步，網路應用產業的安全問題日益明顯，關於協定的惡意攻擊也逐漸增加。ARP（Address Resolution Protocol）是網路傳輸過程中需要使用的通訊協定之一，通過目標設備的 IP 位址，查詢對應的 MAC（Media Access Control）位址，以保證通信的順利進行。由於 ARP 為重要協定之一，因此有許多透過傳遞 ARP 封包的過程或是竄改封包內容來進行攻擊的行為。

本研究將利用模糊測試（Fuzz Testing）的方式（如圖 1）來測試 ARP 有哪些弱點，發現弱點後探討如何避免或防範。雖然模糊測試在概念上易於理解，但在實際的應用方面有較高的難度。

目前我們進度成果如圖 2、圖 3，程式由使用者輸入使用哪個介面卡、來源及目的 IP，之後即可發送 ARP REQUEST 封包。

圖 1：模糊測試步驟

```
tc@sima:~/Desktop$ sudo pytho
n arp-v1\(ubuntu\).py
[sudo] password for tc:
Input Interface:enp0s3
Input Source IP:192.168.1.104

Input Destination IP:192.168.
1.102
tc@sima:~/Desktop$
```

圖 2：程式執行畫面

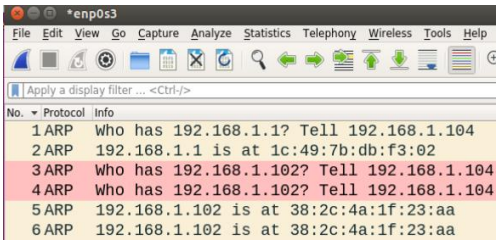

圖 3：Wireshark 封包截取畫面