**網路攻防實務 期末作業**

**班級：資管四甲**

**學號：B0344108**

**姓名：鄭亞欣**

請分析說明以下三種攻擊場景(70%)，並任選以下一個攻

擊場景進行實作(30%)，說明該場景的攻擊原理與建置方

法，並試著實作該場景，此三場景請參考Blackhat

Python一書的第四章。

**(1) 如何從網路流量中竊取Email的密文。可參考Stealing Email Credentials章節 (20%)**

利用sniff函式，去選擇要監聽的封包，可以透過選擇不同的port，過濾掉不需要的部分，以竊取Email密文為例，在監聽的函式中加入過濾條件，將非Email通訊協定用到的port過濾掉，只留下port 110(POP3)、port 143(IMAP)以及port 25(SMTP)，並且透過設定store為零，使監聽的過程中，封包不會留在記憶體中耗能。而當使用者透過以上三種port且使用明文傳送帳號以及密碼資訊時，Scapy便可將其帳號密碼等資訊監聽下來。同時，在函式中也加入判斷條件，如果發現偵測到認證資訊時，就將要傳送目的地主機以及封包內容顯示出來，達到竊取資料的目的。

**(2) 如何透過ARP Spoofing技巧進行內網MiTM的攻擊，可先說明何謂MitM攻擊。可參考ARP Cache Poisoning with Scapy章節 (20%)**

**MitM**：中間人攻擊，透過更改Gateway，將別人的封包先轉給自己，並且竄改其中資料後，在偽裝成原本的傳送者，重新送回到真正的目的地。

透過Scapy，則可以更方便的污染ARP cache，進行MitM攻擊。當資料要從網路進入目標主機時，都需要先進入Gateway，而Gateway會找出ARP cache，裡面包含了區域網路中最新的MAC Address 和IP Address的對應關係，透過查詢以及核對ARP cache，才將資料送入。

想進行MitM攻擊時，就必須透過更改ARP cache中的位址去欺騙Gateway。開始攻擊前，可以先紀錄攻擊目標的IP Address和MAC Address的對應關係，接著再攻擊函式中，先利用get\_mac函式解析Gateway與目標IP位址及其對應的MAC位址開始，同時poison\_target函式會建立污染目標IP與Gateway所需的ARP請求，之後啟動另一個thread實際開始ARP污染攻擊，接著再透過restotre\_target函式，將網路恢復成ARP攻擊前的狀態，而當Gateway與目標IP同時被污染後，就能看到目標主機的傳送及接收的資料內容，並利用回權持續傳送這些ARP請求，確保攻擊過程中，ARP cache一直是被污染的狀態。

**(3) 分析PCAP封包，從PCAP封包中取得HTTP裡面的圖片資料，並將這些圖片資料進行人工智慧比對，快速篩選，若要完成上述功能，需如何透過Python Scapy工具達到？(30%)**

若要分析HTTP的PACP封包中的圖片，需要利用OpenCV電腦視覺工具幫忙，透過這個工具，可以偵測封包中是否有含人臉的圖片，過濾出較有利用價值的圖片，而PCAP檔，可以利用前面的ARP Poising產生，或是擴充ARP Poising程式，使它在執行時，就能夠即時偵測是否有人臉圖片在封包當中。

**實作：**

本來想嘗試利用PCAP封包，進行圖片的比對，但後來因為沒做ARP Poising，而Wireshark攔截到的封包，程式一直無法找到檔案，所以就改做第一個。

第一個的程式碼主要只有改變監聽的port number，不是以Email通訊協定，而是改成tcp port 80以及tcp port 21為主，成功在封包中抓到透過未加密網站登入時的帳號密碼。以下是操作過程，附件是執行過程的影片。

GitHub：<https://github.com/SunnyCheng1125/Final-report-code>

