



亞洲大學 | 健康 · 關懷 · 創新 · 卓越
ASIA UNIVERSITY

資安防護之社交工程演練系統

亞洲大學 資訊工程學系
周悅鵬 邱詣函 林宗彥 黃泓儒



- 此社交工程演練系統主要是透過發送電子郵件來誘使受測對象點擊連結，從而紀錄受測對象的存取行為，以分析企業或組織的防護漏洞，透過取得數據來了解演練成效。
- 對一些學生或是企業的人員來說，電子郵件社交攻擊將導致後門程式被植入內部電腦，會聽到的反應卻是；「好像很嚴重，但不知道具體的嚴重性有多大。」從而忽略此防護漏洞可能帶來的巨大風險。本計畫能夠提高警覺性以降低社交攻擊風險，以此來強化人員資安意識並且檢驗社交工程防治宣導的成效。



實作背景與動機

- 根據台灣網路資訊中心所公布「2017台灣寬頻網路使用調查」報告，全國12歲以上使用網路的人口數已達1,760萬人，全年齡人數約為1,879萬，相當於百分之80左右。人們的生活對網路已有高度依賴信，不過網路發達帶來方便的同時也帶來一些風險。
- 在網路日漸發達和通訊軟體普及的時代詐騙手法越來越多，開始出現使用電子郵件進行網路攻擊，有心人士利用社交工程的技巧針對人性弱點，例如:好奇、恐懼、貪婪、同情、信任感等等，欺騙受害者點擊郵件中的不明連結或惡意程式碼，藉此植入病毒或惡意程式。



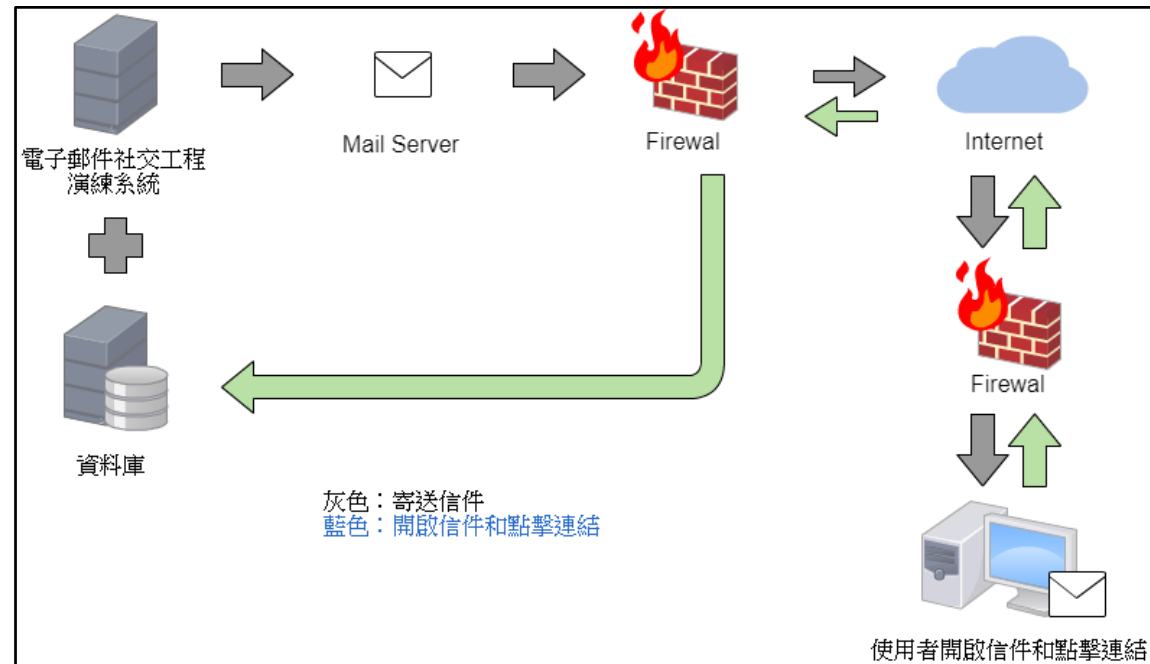
實作背景與動機

- 社交工程演練是透過模擬駭客寄出攻擊信件，用聳動吸引人的內容和標題去引誘受害者打開郵件，以達到攻擊演練動作，針對每次演練結果統計去觀察在何種情況下受害者較容易開啟郵件。



計畫目的與範圍

- 目前我們計畫透過模擬演練電子郵件社交工程，我們將分出特定3種情況（例如：一般、個人、公務）隨機發送其中一類郵件，我們將收件者點開郵件紀錄做整理，分析受到攻擊之對象通常在什麼時間，會開啟信件或點擊連結的動作。

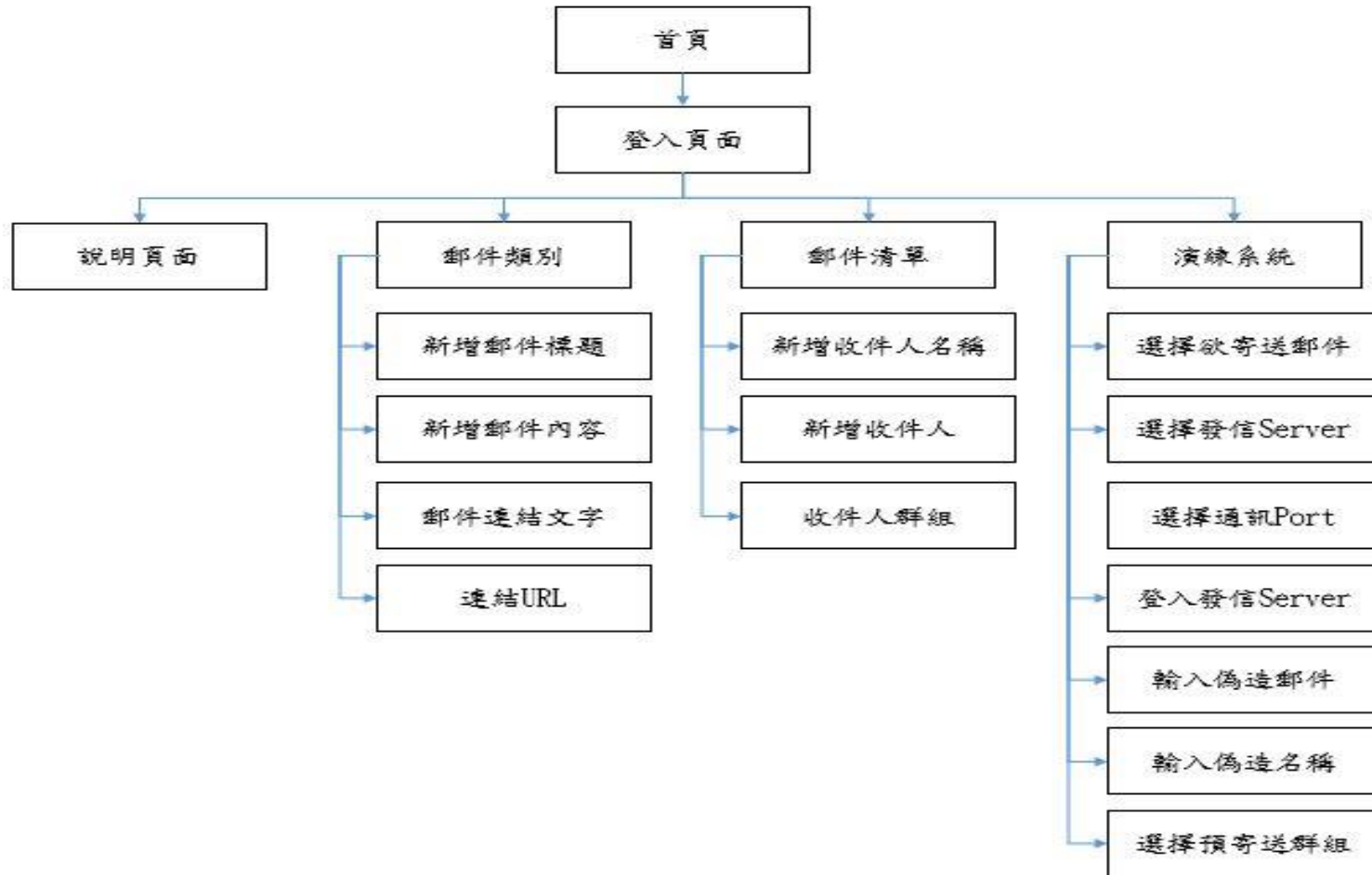


環境需求

硬體	
桌上型電腦	CPU3.2GHz/記憶體8GB/硬碟512GB
防火牆	Fortigate 80C
作業系統版本	
DNS Server	Bind 9.9.4
Mail Server	發信：Postfix 2.10.1 收信：Dovecot 2.2.10
WWW Server	Apache 2.4.6 (CentOS)
資料庫	phpMyAdmin 4.0.10.20
寄信演練系統	PHPMailer 6.0.1
撰寫程式工具	
Web	Brackets



網站架構圖



外網發信實測

```
[peng@mail ~]$ mail c23933287@gmail.com
Subject: testing mail
test
.
EOT
```



從Mail Server使用mail指令進行發送郵件，輸入主旨以及信件內容，最後輸入“.”表示信件編輯結束，發送完畢並至Gmail信箱查看信件，確認是否收到信件，檢查時間及主旨是否相同



外網收信實測

```
周悅鵬 <c23933287@gmail.com>  
寄給 peng ▾  
test part 2  
2017-12-04 0:38 GMT+08:00 <peng@anquan304.idv.tw>:  
| test
```

```
5 N Dec 04 周悅鵬 ( 22) Re: testing mail
```

```
Date: Mon, 4 Dec 2017 00:40:22 +0800  
From: 周悅鵬 <c23933287@gmail.com>  
To: peng@anquan304.idv.tw  
Subject: Re: testing mail  
  
test part 2  
  
2017-12-04 0:38 GMT+08:00 <peng@anquan304.idv.tw>:  
  
> test  
>
```

從Gmail回信至Mail Server，
輸入信件內容並發送信件
至Mail Server的mailbox查看信件是否寄發並收到
Mail Server使用mutt軟體來管理信件，開啟信件並
確認時間和內容是否相同





歡迎使用者[登出]

說明頁面 郵件清單 郵件類別 演練系統

資料	群組名稱	刪除	
顯示	亞洲大學	刪除	<input type="text"/> 匯入檔案
顯示		刪除	收件人名稱: <input type="text"/>
顯示		刪除	收件人郵件: <input type="text"/>
顯示		刪除	收件人群組: <input type="text"/>
顯示		刪除	<input type="button" value="確認"/>
顯示		刪除	





歡迎使用者[登出]

說明頁面 郵件清單 郵件類別 演練系統

郵件類別:

新增類別

編輯	郵件類別	信件標題	刪除

信件標題:

信件內容:

替代文字:

連結:



演練系統



歡迎使用者[登出]

說明頁面 郵件清單 郵件類別 演練系統

郵件標題:

郵件伺服器:

伺服器通訊埠:

寄件者帳號:

寄件者密碼:

偽造郵件:

偽造名稱:

收件群組:

Submit



系統實作成果 DEMO





亞洲大學
ASIA UNIVERSITY



Q&A

THANKS!

