中華大學資訊工程學系
105 學年度專題製作期初報告

OpenFlow 網路攻防模擬

指導老師：王俊鑫 教授

組員：陳書慕(B10302042)

中華民國 105 年 3 月 10 日

壹、專題計畫摘要：於本專題要點做一概述。

我這組所作的專題是網路攻防模擬，由於現在網路攻擊方式層出不窮，像是：DDoS 攻擊、SQL Injection、XSS 攻擊、Phishing 釣魚....等，而這些攻擊方式，大部分的防範方法都是被動的。而我這次的專題，是想要直接從網路封包上，觀察出每一個封包的內容，並且當收到惡意封包後，直接處理該封包。如此一來，電腦就不會受到網路攻擊了。

貳、背景及目的：詳述本專題之背景、目的、重要性。

背景：利用 omnet++這個網路模擬開發環境，並且用 Openflow 來作爲網路拓樸，然後模擬網路上惡意封包攻擊的網路環境。

目的：爲了防止電腦遭受到網路攻擊，而不再被動的等被攻擊才有防範方法。

重要性：當電腦遭受到網路攻擊的時候，往往電腦都無法作業，或是被別人更改資料內容。因此，網路上的安全是不可忽視的。

參、專題內容：

透過 omnet++模擬網路環境，並且觀察當電腦遭受到網路惡意攻擊，是否能夠判斷哪些封包是正常的，哪些是不正常的，然後用 Opneflow 來完成網路的拓樸。

肆、專題研究方法及進行步驟：

1．細述專題採用之研究方法與原因。

將採用 omnet++網路模擬開發環境，來模擬在 openflow 拓樸下的網路遭受到網路攻擊

開發環境：omnet++

初期：主要研究 omnet++的模擬環境、模擬語言，以及 openflow 的結構與概念

中期：收集資料，網路拓樸，程式撰寫，觀察網路傳輸狀況

後期：紀錄網路封包傳輸

2．預計可能遭遇之困難及解決途徑。

有可能遇到的困難：

1．模擬環境：第一次接觸 omnet++的模擬環境在 使用上還需要熟悉

2．程式語言：雖然大部分都是由 c++撰寫，但有需要在學習

3．Openflow：有許多網路上的概念與知識需要學習，並且了解何謂 SDN

重要儀器爲：

1．模擬環境所使用的電腦

2．儲存程式碼與資料的硬碟或空間

伍、預期完成之工作項目及具體成果:

第一部份：了解何謂 openflow 與熟悉 omnet++

第二部份：設計網路拓樸與網路攻擊方式

第三部份：觀察與紀錄網路封包狀況

第四部份：成果發表

陸、預定進度甘梯圖:

月份 工作項目	第1月	第2月	第3月	第4月	第5月	第6月	第7月	第8月	第9月	第10月	第11月	第12月
專案設計												
收集資料												
專案規劃												
熟悉語言												
網路拓樸與 程式撰寫												
觀察網路環境												
除錯 回報												

柒、儀器設備需求表

1. 撰寫程式的電腦

捌、參考文獻

1. Software Defined Networking(DESIGN AND DEPLOYMENT)

作者：**Patricia A. Morreale、James M. Anderson**

出版社：**Taylor & Francis Group, LLC**

出版日期：**2015**