Final Project Proposal

林峻賢 0711540

1. 題目：IP Spoofing模擬攻擊與防禦
2. 動機

網路的誕生為了讓使用者可以更方便的與人交流資訊，因此設計之初的架構並未防範惡意攻擊，所以壞人可以透過這些漏洞進行惡意傳送封包，導致網路發生壅塞或癱瘓。在歷經數十年的攻擊與防禦後網路架構更加安全，而IP spoofing是時至今日仍然流行的攻擊手段之一，為了瞭解這個攻擊手段原理如何運作以及防範，我希望能藉由這個期末專題徹底理解，並實際應用課堂上學習的知識。

1. 實驗流程

建立三台linux虛擬機分別做為attacker、server、victim client。Victim client首次與server建立連線時，attacker要設法去監聽到client的source MAC address、source IP、destination IP等等的相關資訊，attacker知道以上這些資訊之後便可製作spoofing packets，將這些spoofing packets送給server，server將會認為這些封包應屬於victim client發送的而將對其進行回應，而這樣便可以對client進行一輪的攻擊。

|  |
| --- |
|  |
| 圖一 |

如圖一所示，attacker以竊取得到的資訊製作出spoofing packets會送往routers進行forwarding，spoofing packets抵達server所處，server便對其做出回應，但收到response packets是victim client。

要對IP spoofing進行防禦可以使用packet filtering，針對封包的source IP與實際IP不符時拒絕傳送。預計會使用Python實作，並且使用scapy package製作spoofying packets。

1. 參考資料
2. [Day 17 網路層攻擊實例 - IP Spoofing - iT 邦幫忙::一起幫忙解決難題，拯救 IT 人的一天 (ithome.com.tw)](https://ithelp.ithome.com.tw/articles/10248149)
3. [DDoS防禦 - 海爾雲端 (highercloud.com.tw)](https://www.highercloud.com.tw/service-ddos?%2Fservice-ddos)