# Midterm

Test Time: 2016/4/20 (Wed.) 18:30 入場

## Instructions and Announcements

- 考試時間共三小時，三人一組依照座位分配坐在一起，每組有 R204 的兩台新電腦和一台舊電腦可以使用。
- **所有題目請在 R204 的新電腦 上完成，不可以使用自己的筆電作答**，但可以使用筆電或舊電腦查詢資料。
- 為避免發生重大意外，請自行在過程中斟酌是否需要備份 VM。若真的不幸發生悲劇，助教可以提供原始狀態的 VM，但傳輸或下載 VM 需花費一些時間，請盡量避免此一情況。
- 除第 6 大題外，完成題目時可使用**召喚助教**召喚助教過去評分。
  如果還沒完成就偷跑先召喚助教，會給予 penalty 2pt。有結果可以 demo 但 demo 失敗不在此限。助教有權判斷並決定是否給 penalty。
- 組與組間**禁止討論**，如被發現視為作弊行為，**期中考 0 分**。
- 各題後面黑色星號數目代表我們估計的難度。請參考，可用來決定解題順序。
- 滿分 200pt，另有 bonus 20pt。
- Good Luck!!

# 1 Traffic analysis using Wireshark (10 pt) ★☆☆☆☆

Given the file **traffic.pcapng**, please answer the following questions:

1. Which devices had possibly been involved in port-scanning attack(s)? Find the IP addresses and MAC addresses of all attackers and victims. (3 pt)
2. Please filter out every ARP request in VLAN 5 between the time 2016-4-13 14:09:00 and 2016-4-13 14:10:00. Save the filtered packets to a separate .pcapng file. (4 pt)
3. Please determine which device had pinged 8.8.8.8, successfully got the reply, and had logged into PTT server via SSH. Find its IP address and MAC address. (3 pt)

## 2 Cisco Basics (20 pt) ★★☆☆☆

以下 <tid> 為組別編號 (01-19)，請自行取代成自己的組別。請以 SSH 連線到 10.8.0.4，帳號密碼皆為 team<tid>，登入後進行以下操作：

1. 修改自己的密碼 (只要不是預設密碼就可以)(4 pt)
2. 對於 interface Gi0/<tid> 做以下設定：
   - 移除原本的設定 (4 pt)
   - 將介面敘述設為 team<tid> (在 user mode 及 privileged mode 可以用 `show interfaces status` 指令看到) (4 pt)
   - 將該介面設為 trunk (4 pt)
   - trunk 只允許 VLAN <100 + tid> 以及 VLAN 252 通過 (4 pt)

### Warning and hint

- 下指令前請三思，**嚴禁修改別組設定或是做題目範圍以外的設定**。違反者**本題 0 分**。
- 由於 switch 僅允許 15 個 users 同時登入，**設定完成後請記得登出**。
- 有些指令上課沒教，請善用?、<Tab>、課堂投影片以及 Google。
- 上課有說過，Cisco 的設定檔就是指令。

# 3 Firewall and DNS

你會用到的 VM：pfSense, Lubuntu*2，root 密碼:nasa2016

## 3.1 Firewall (30 pt) ★★★☆☆

你是一家公司的網管。每天員工們都可以在上班時間愉快的上網。有一天老闆覺得員工上班用 facebook 的問題頗為嚴重，要求你不讓員工連上 facebook(www.facebook.com)。不過因為生意上的需要，老闆還是要能上 facebook。

1. 切 vlan2(192.168.2.254/24) for 員工和 vlan99(192.168.99.254/24) for 老闆。VLAN 和之前作業一樣是 802.1Q 的 tagged VLAN，一樣要自己在 Lubuntu 上生 interface。(3 pt)
2. vlan2 與 vlan99 都能正常上網，不必背 IP，也不必設定自己電腦的 IP。但是 vlan2 不能用 https 連上 facebook，vlan99 可以。(9 pt)
3. 為了維護老闆電腦的機密資料，vlan2 碰 (ping and ssh) 不到 vlan99 的電腦。但是 vlan99 碰的到 vlan2 的電腦。(6 pt)
4. 老闆想從國外也能連回自己的電腦工作。請嘗試使 windows 可以 ssh 到防火牆後面 vlan99 老闆的電腦。(12 pt)

**Hint**

- windows 碰不到 Lubuntu，只碰的到 pfSense。想辦法讓 windows ssh pfSense 的 port 12345 時，實際上可以連到 Lubuntu 的 port 22。
- You might need to use `port forwarding`。
- 這次 pfSense 對外的網卡和電腦是 bridge 不是 NAT。
- 需要改 DNS 的話可以直接改 Lubuntu 的設定檔。

## 3.2 DNS (30 pt) ★★★☆☆

1. 老闆突發奇想請你架一台公司自己的 DNS 伺服器，請幫助他架設並且設定讓老闆的電腦和員工電腦使用這台 DNS 伺服器。(公司資源有限，沒有多的伺服器可以用，所以聰明的網管你只好幫老闆把 DNS 伺服器架在老闆的電腦上。) (9 pt)
2. 為了避免往後可能產生不必要的麻煩，請不要讓 vlan2, vlan99 網段以外的 IP 可以透過這台做 DNS 查詢。(Hint: `allow-recursion`) (9 pt)
3. 老闆受夠難記的 ip 了，請幫他在 DNS server 上設定 “boss.nasagroup<Group ID>.com” 指向老闆的電腦，以及 “employee.nasagroup<Group ID>.com” 指向員工的電腦 (6 pt)
4. 老闆請你幫員工的電腦設一個別名叫做 “e.nasagroup<Group ID>.com”，想必是因為老闆想要節省寶貴的時間而不是記不得 employee 怎麼拼。你有種預感，性格古怪的老闆之後很有可能會再請你幫他設定其他別名，為了維護方便，請將別名全部指向最初設定的 domain name 而不是 IP 位址。(6 pt)

**Hint**

- 請就 VM 當時拿到的 ip 設定，不需要考慮之後可能會拿到不同 ip 的情形

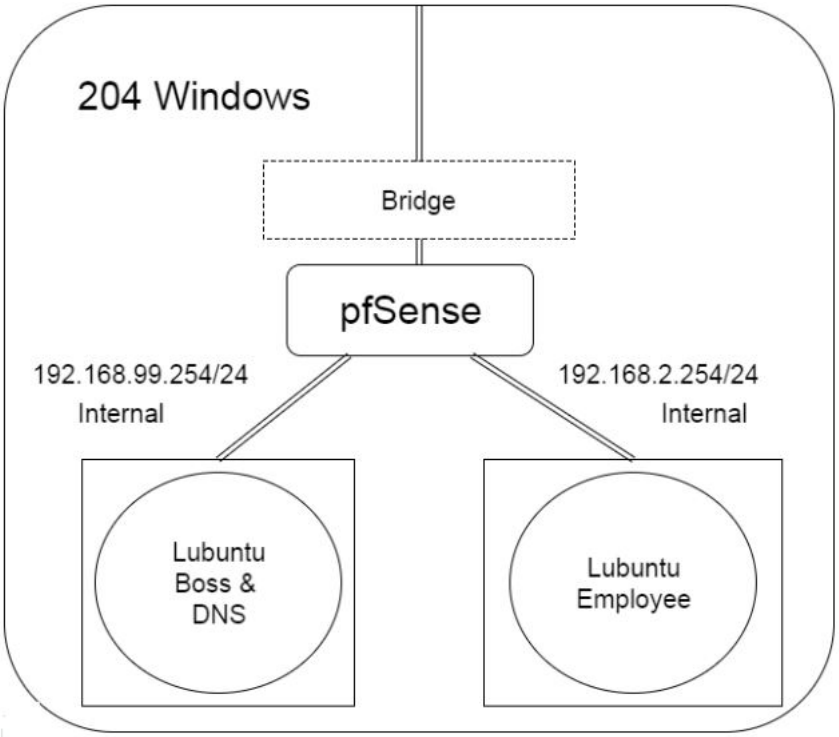


Figure 1: VM Structure

# 4 SSH (40 pt) ★★★★☆

你會用到的 VM：Lubuntu(你可以使用第三大題的其中一台 Lubuntu，或是開一台新的 Lubuntu)

1. SSH public key authentication (6 pt)
   使用 SSH 連線到遠端主機時，除了可以使用密碼登入，也可以使用公鑰認證登入。在這個題目裡，我們要用公鑰認證登入工作站。請產生一組公鑰和私鑰，其中公鑰必須要上傳到工作站上，而私鑰則要妥善保管，不可以讓別人知道。
   - 金鑰類型必須是 RSA 3072-bit 以上，或是 ECDSA 256-bit 以上，不可以用 DSA。
   - 三個人分別要產生三組金鑰，分別用於登入三個人的工作站帳號。
   - 私鑰檔名不可以是 `~/.ssh/id_rsa` 或 `~/.ssh/id_ecdsa`。
   - 私鑰必須設定密碼，不可以明文存在硬碟上。
2. SSH local forwarding (10 pt)
   SSH 除了可以在遠端主機上執行指令，也可以將遠端主機才能連上的 port 轉回給本機，讓本機的程式透過遠端主機間接連上服務。在這個題目裡，我們要使用本機的 telnet 程式連上只有工作站才能使用的 echo server。
   - 使用 SSH 連線到工作站上。
   - 在本機執行 `telnet localhost <某個自己指定的 port>` 必須要能透過工作站連到 `intern.csie.ntu.edu.tw:7`。
3. SSH remote forwarding (10 pt)
   SSH 不只可以將遠端的服務轉回給本機的服務使用，也可以將本機的服務轉給遠端主機使用。在這個題目裡，我們要讓遠端主機可以連線回本機。
   - 本機安裝並啟動 SSH 伺服器。
   - 使用 SSH 連上到工作站上。
   - 能在工作站透過自己指定的 port 用 SSH 連線回本機。
4. SSH SOCKS proxy (14 pt)
   如果我們有很多服務必須要透過遠端主機的網路才能存取，透過 local forwarding 功能把每個要使用的 port 都轉送回本機是一大麻煩。這時候可以請 SSH client 在本機啟動一個 proxy server，這樣我們只要指定要使用的 proxy server 就能連上遠端服務。
   - 使用 SSH 連上到工作站上。
   - 設定瀏覽器使用本機上 SSH 啟動的 proxy server 來對外連線。
   - 連線到 https://icanhazip.com/，確認顯示的 IPv4 位址是工作站的。

## 以下是 Bonus!! (20 pt)★★★★★

5. 透過 SSH 使用 Git 版本管理軟體 (8 pt)
   現在有很多應用程式支援透過 SSH 來加密傳輸資料，但是這也代表有些時候你無法控制 SSH 指令執行使用的參數，因為 SSH 是由應用程式啟動，而不是你手動輸入指令執行的。這時候為了讓 SSH 能用正確的設定執行，就必須要將設定值存在設定檔才行。
   - 三個人分別在自己的工作站家目錄開新資料夾並建立空白的 git repo (`git init --bare`)。
   - 修改本機的 `~/.ssh/config`，指定不同使用者執行時要使用的公鑰。

- 在本機執行 `git clone ssh://user@host/path/to/git/repo` 指令，三個人的 git repo 都必須能成功下載到本機，而且是用公鑰認證連線到工作站。

6. SSH agent (6 pt)
   你可能已經開始覺得，每次都要輸入私鑰密碼才能連線到遠端主機，使用起來很不方便。事實上我們可以透過一種稱為 SSH agent 的程式，把解密後的私鑰暫時存著在記憶體中。我們只需要事先告知 SSH agent 會使用到私鑰和密碼，SSH agent 就能在 SSH 執行時協助完成認證，而不需要每次連線都輸入解密密碼。

   - 在本機執行 SSH agent，並確認存放 socket 檔的資料夾只有現在的使用者可以存取。
   - 將可連線到工作站的私鑰加入 SSH agent。
   - 確定可以不用輸入任何密碼就連上工作站。

7. SSH agent forwarding (4 pt)
   有些時候我們會需要在遠端的機器上使用 SSH，但是我們通常不會想要把本機的私鑰傳送到遠端主機上，因為對外開放的機器比較容易遭受攻擊，系統安全設定也不一定是我們可以控制的。這時候我們有一種風險較低的處理方法：將本機 SSH agent 的 socket 暫時轉送給遠端機器使用，讓遠端機器在無法存取私鑰檔的情況下仍能使用 SSH。

   - 在本機執行 SSH 並將可連線到工作站的私鑰加入。
   - 在工作站上可以免密碼登入其他臺工作站。

8. SSH askpass (2 pt)
   有些使用 GUI 的應用程式雖然有支援使用 SSH，但是並沒有提供輸入登入用密碼或解鎖私鑰密碼的視窗。如果我們沒有事先設定好 SSH agent，就可能會因為 SSH 無法讀到密碼而登入失敗。這時候我們可以請 SSH 使用指定程式顯示視窗，改用 GUI 輸入密碼。

   - 關閉 SSH agent。
   - 執行 `setsid ssh user@host -- cat /etc/motd`，不可自行增減任何參數。
   - 可以在不透過終端機輸入密碼的情況下成功登入，並看到工作站的登入訊息。

# 5 System Administration

你會用到的 VM：Lubuntu(你可以使用第三大題的其中一台 Lubuntu，或是開一台新的 Lubuntu)

## 5.1 Shell Script (20 pt) ★★☆☆☆

請寫一個 script 列出目前每一個 uid 各有幾個 process (不用考慮 threads)
輸出格式：每行一個 <uid> <num_process>

Example output:

```
0 100
102 1
124 1
41610 217
```

## 5.2 Storage (30 pt) ★★☆☆☆

1. 請在 Virtualbox 新增兩個 1GB 磁碟，並建立一個符合以下條件的 RAID：
   - RAID 1
   - ext4

   磁碟中的資料必須要在移除一個磁碟後仍然可以正常存取。
2. 新增另一個 1GB 磁碟，並加密它。
3. 設定使得前二題中的磁區能在開機時被 mount。Mount 的目錄請自行決定並創建。

# 6 Debug!? (20 pt) ★★★★☆

現場將會有總共五台不能連網的機器，請想辦法找出問題並修復，讓他可以恢復正常上網。每組只需破解一台機器即可拿到 20 pt。每組將會有最多兩次挑戰機會，一次 15 分鐘。五台機器是各組輪流共用，詳細挑戰時刻表請看當天白板。同一時段會有五組同時挑戰，當場才會抽籤決定各自拿到哪台機器。

如果對規則有任何問題請隨時召喚助教。