交通大學 計算機系統管理 109學年度上學期 期末考

NCTU Computer System Administration 109A Final Exam

Date/Time: 2020/12/31 PM 06:30 ~ 08:30 (2 hours)

Open Book, No Electronic Equipment

Assume the operating system is FreeBSD 12.1-Release

English follows Chinese in every question. Both Chinese and English answers are acceptable.

========== Questions start from here ==========

Part A: Multiple Choice (2% each, total 14%, 7 questions)

1. 請問下列何者無法透過 PF 與 iptables 來過濾？
   Which one cannot be filtered by PF/iptables?

   (A) TCP Flag (B) HTTPS (C) MAC Address (D) IPv6 Address

2. 請問所謂的Privileged Ports是TCP/IP Port number小於哪一數字的Port？
   "Privileged Ports" are TCP/IP ports that have a port number less than which number?

   (A) 512 (B) 1024 (C) 2048 (D) 768

3. 請問採用TLS/SSL加密的連線建立後，資料傳輸是使用哪一個加密演算法？
   Which cryptosystem is used for data transmission after the connection is established in TLS/SSL?

   (A) 非對稱式加密。
   Public-key cryptosystem.
   (B) 對稱式加密。
   Symmetric-key cryptosystem.
   (C) 不加密。
   No encryption.
   (D) 以上皆非。
   None of the above.

4. PF 的 Tables 描述如下，請問下列哪一選項不符合此 Table 設定？
   Assume we have a PF Table entry below. Which following address does not meet the condition of this Table?

```
table <hosts> { 140.113.0.0/16, !140.113.121.0/24, 140.113.121.108/29 }
```

   (A) 140.113.23.12 (B) 140.113.123.4 (C) 140.113.121.112 (D) 140.113.121.107

5. 下列哪一個**不是**向 CA（Certificate Authority）申請憑證所需提供的資訊？
   To request for certification from CA(Certificate Authority), which one below is NOT required?

   (A) 公鑰。
   Public key.
   (B) 憑證請求檔。
   Certificate request.
   (C) 私鑰。

Private Key.

(D) 身份（公司、組織）證明文件。
ID proof of your organization.

6. 下列對於TCP的描述何者正確？
Which description is suitable for TCP?

(A) 不具備 Connection 的觀念。
It is connectionless.

(B) 傳輸不可靠。
It is unreliable.

(C) 不具Data Checksum。
It does not have "Data Checksum".

(D) 具Flow Control。
It has "Flow Control".

下列哪一個程式可對 log 檔進行 rotation 或壓縮等管理功能，以避免 log 檔無限制地增長？
Which utility can be used to rotate or compress the log files?

(A) rsyslogd (B) periodic (C) rsync (D) newsyslog

Part B. Short Answer (total 86%, 17 questions)

1. (4%) Autofs Client
   A. (2%) 如果想要掛載 NFS伺服器「ccstorage」於 /share資料夾下分享的所有子目錄（例如 /share/www與/share/data等），試問如何只使用一條 indirect map 的規則來達成，而不需要列舉所有子目錄名稱？ * -nfsv4 ccstorage :/share/ &
   Assume we want to mount all subdirectories exported by NFS server "ccstorage". For example, we want to mount directories "/share/www" and "/share/data". Please describe how could we use just ONE rule in indirect map to achieve this without enumerating all subdirectories.

   B. (2%) 如果網路中有兩台 NFS 伺服器「ccstorage」與「ccweb」，試問該如何設置 master map 使得我們可以只用一條規則，便讓 /net/ccstorage目錄底下看到所有 ccstorage 分享的所有目錄，以及 /net/ccweb 目錄底下看到所有 ccweb 所分享的目錄，而不需要額外新增 direct/indirect map？
   Assume there are two NFS servers in the network: "ccstorage" and "ccweb". Now we want to mount all directories exported by these hosts. For example, "/net/ccstorage" contains all directories shared by the server "ccstorage" and "/net/ccweb" contains those of "ccweb". Please explain how to achieve this with just ONE rule in master map without using extra direct/indirect maps.

2. (4%) 試比較 microkernel 與 monolithic kernel 兩者的優劣。請就模組化設計程度、最佳化程度、kernel 大小作討論。 /net -host -nosuid,soft
   Please describe the pros and cons of "microkernel" and "monolithic kernel" respectively. You should focus on "modularization", "optimization" and "size of kernel".

3. (4%) Autofs Replicated Filesystem
   A. (2%) 請說明 autofs 提供 replicated filesystem 功能用途為何？
   Please describe the functionality of the "replicated filesystem" in autofs.

B. (2%) 承上，使用 replicated filesystem 有什麼限制？為什麼？
Continued from the above question, what is the main restriction of "replicated filesystem"? Please explain why it has such restriction.

4. (4%) Backup

A. (2%) 請說明 full backup 與 incremental backup 的差異。
Please describe the difference between "full backup" and "incremental backup".

B. (2%) 在還原資料的時候，只有 incremental backup 是否足夠？不足的話還需要什麼？執行還原的順序為何？
Is it sufficient to restore data with incremental backup? If not, what else is needed? What is the order of restoring?

5. (2%) 請解釋 PF 的 block policy 中，drop 與 return 的差異。請分別以TCP與UDP 的角度來解釋。
Please explain the difference of "drop" and "return" when configuring the block policy of PF. You should answer this question in both use cases of TCP and UDP.

6. (6%) Address Resolution Protocol (ARP)
A. (2%) 請說明ARP的用途為何？
Please describe the functionality of "ARP".

B. (2%) 請說明complete與incomplete ARP entry的差異。
Please describe the difference between "complete ARP entry" and "incomplete ARP entry".

C. (2%) 承上，為什麼incomplete ARP entry也需要被記錄？
Continued from the above question, why incomplete ARP entries are still recorded instead of being dropped?

7. (2% each, total 6%) 下列為/etc/syslog.conf的部份內容。
Part of the "/etc/syslog.conf" is attached below.

```
*.err;*.alert;kern.warning;auth.notice;mail.crit;lpr.none      /dev/console      ❶
*.notice;authpriv.none;kern.debug;lpr.info;mail.crit          /var/log/messages ❷
*.alert;kern.crit;local5,local6,local7.info;local7.none       root              ❸
*.*                                                           @loghost          ❹
```

當下列logging事件發生時，會被記錄至哪裡地方？（答案可能不只一個地方，回答時填入編號❶❷❸❹即可）
What are the logging destinations (may more than one) for following logging events? Answer in numbers ❶, ❷, ❸ or ❹.

A. user.err 41
B. lpr.notice 42
C. local7.info 43

8. (4%) setuid 的 script 通常會有較高的安全風險，為什麼？系統管理者可以從檔案系統的角度用什麼方法降低風險？

There is more high security risk with setuid scripts. Please explain the reason and propose a solution to reduce the risk (from the filesystem side).

9. (8%) Device and Kernel
   A. (2%) 當某裝置的驅動程式 (device driver) 在當前 kernel 並不支援，除了重新編譯 kernel外，請問尚有什麼方法可讓 kernel 支援此裝置？
   If the driver of a device is not supported in the current kernel, is there any approach to support this device WITHOUT recompiling the kernel?

   B. (2%) 承上，重新開機後是否仍支援此裝置？為什麼？
   Continued from the above question, is that device still supported after system reboot? Why or why not?

   C. (2%) 欲將每個 UID 允許Process數量設定為 20000，請問如何在不重新啟動主機的狀況下更改該 kernel 變數？請寫出完整的設定指令及參數。提示：該變數名稱為「kern.maxprocperuid」。
   To change the max process number per UID, we can change the kernel variable "kern.maxprocperuid". Please describe how to set this value to 20000. You need to write down the detailed commands and their parameters/options.

   D. (2%) 承上，若主機重開後需繼續套用該數值，該如何實現？
   Continued from the above question, how could we keep this configuration working after rebooting without running above command every time?

10. (2%) 請說明使用 autofs 比起傳統的 /etc/fstab，有什麼好處？
    Please explain why using "autofs" is better than traditional "/etc/fstab".

11. (10%) Web
    A. (2%) 請問 web Server 是利用 HTTP header 中的哪項資訊識別以提供 Name-Based Virtual Hosting 功能？
    Which field of HTTP header is used to implement the "Name-Based Virtual Hosting" in web servers?

    B. (2%) 請問若 web server 採用 self-signed 的憑證，為什麼瀏覽器連上時會跳出警告訊息為不受信任的網站？在**不更換憑證**的前提下，該如何解決此問題？亦即，請想像你只是使用者而非該伺服器的管理者。
    Why do browsers show "untrusted websites" when connecting to a web server that uses a self-signed certificate? How could we address this issue **WITHOUT** changing the certificate? In other words, you are the user and the web server still used that self-signed certificate.

    C. (2%) 請問要如何讓 Apache 的 Name-based Virtual Hosting 功能支援 SSL/TLS？
    Please propose a solution to support SSL/TLS for "Name-based Virtual Hosting" in Apache web servers.

    D. (2%) 請說明 Name-Based Virtual Host 與 IP-Based Virtual Host 的差異。
    Please explain the difference between "Name-Based Virtual Host" and "IP-Based Virtual Host".

    E. (2%) 承上，若提供網頁代管服務通常會採用哪一種技術？為什麼？
    Continued from the above question, which technique is suitable for providing web hosting services? Please explain why.

12. (4%, 1% each) 給予一段IP address：140.113.55.66/28，試回答下列問題（請用十進位表示，例如

X.X.X.X）。
Given an IP address subnet "140.113.55.66/28", please answer the questions below (in Decimal representation, like format of X.X.X.X).

A. 子網路遮罩是多少？
What is the Netmask?

B. 此網路的 Network ID 是多少？
What is the Network ID?

C. 廣播位址是什麼？
What is the Broadcast Address?

D. 實際上總共有多少可使用的IP Address？
How many IP addresses are available for assigning to hosts in this network?

13. (2%) 當主機的 /etc/hosts與NIS的hosts map皆具有同一台主機名稱對應的IP Address設定，請問系統是根據哪一個系統檔案的設定來決定查詢順序？
If a hostname entry exists in both /etc/hosts from localhost and hosts map from NIS, which system file specifies the priority of the two?

14. (4%) 請解釋以下 PF 規則所代表的涵義是什麼。請以兩個不同的 IP「10.0.0.1」與「10.1.2.3」的角度來解釋。
Please explain the meaning of following PF rule. You should use two different IP addresses "10.0.0.1" and "10.1.2.3" to answer this question.

```
pass out on fxp0 to { 10.0.0.0/8, !10.1.2.3 }
```

15. (total 10%) Database
A. (4%) 請解釋 MariaDB 與 MySQL 之間的關係。
Please explain the relation between MariaDB and MySQL.

B. (6%) 當使用這類型 Open Source 軟體遇到問題的時候，有什麼方式可以尋求協助，包含免費與付費的方案。
If you have problems with open source software like MariaDB or MySQL, do you have any method to find the support, including free and paid solutions.

16. (total 6%, 2% each) 請舉出至少 3 個 Firewall 的應用場景。
Please propose (at least) 3 scenarios of firewall usages.

17. (6%) 請簡述 Certificate Pinning 及此機制可以避免什麼樣的攻擊。
Please briefly describe what certificate pinning is, and what type of attack does it prevent?

64 + 15 = 79
0 1 0 0 1 1 1 1
1 1 1 1 - - - -
128 64 32 16 8 4 2 1

128
64
192
32
229
16
240