

交通大學 計算機系統管理實務 2020 期末考
NCTU Computer System Administration Final Exam

Date/Time: 2020/01/09 PM 06:30 ~ 08:30

Open Book, No Electronic Equipment

Assume the operating system is FreeBSD 12.0-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 16%, 8 questions)

1. 下列哪一個程式不應該給予 setuid 權限？

Which program should not have "setuid" permission?

(A) /usr/bin/chfn (B) /usr/bin/chsh (C) /usr/bin/passwd (D) /usr/bin/w

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 port number less than which number?

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

3. 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".

4. 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 above

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. 請問若 master.passwd 欲存取 NIS 資訊時，需新增下列哪一行至檔案的最後面？

In order to let "master.passwd" access the login entry from NIS, we need to append which one to the end of the file?

- (A) \$:*:.....
- (B) @:*:.....
- (C) &:*:.....
- (D) +:*:.....

7. 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) IP Address
- (B) ICMP Type
- (C) TCP Port
- (D) MAC Address

8. 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

Handwritten calculations for option D:
140.113.121.107
140.113.121.0/24
140.113.121.108/29
140.113.121.107 is in the excluded range 140.113.121.0/24, so it does not meet the condition.

Handwritten calculations for option C:
140.113.121.112
140.113.121.0/24
140.113.121.108/29
140.113.121.112 is in the excluded range 140.113.121.0/24, so it does not meet the condition.

Handwritten calculations for option B:
140.113.123.4
140.113.0.0/16
140.113.123.4 is in the range 140.113.0.0/16, so it meets the condition.

Handwritten calculations for option A:
140.113.23.12
140.113.0.0/16
140.113.23.12 is in the range 140.113.0.0/16, so it meets the condition.

Part B: Short Answer (total 84%, 14 questions)

1. (4%, 1% each) 給予一段 IP address : 140.113.55.66/26，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 "140.113.55.66/26", 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?

2. (8%) dump 可用來將 filesystem 備份成檔案或至外部裝置，並支援 incremental 備份，如下為 /etc/dumpdates 檔案內容。請回答以下問題。

The "dump" command can backup filesystem into files or to external devices. It also supports incremental backup. Following is the content of /etc/dumpdates. Please answer following questions.

/dev/ada0p3	0 Thu Jan 06 00:30:00 2019	①
/dev/ada0p3	2 Fri Jan 07 00:30:00 2019	②
/dev/ada0p3	1 Sat Jan 08 00:30:00 2019	③
/dev/ada0p3	3 Sun Jan 09 00:30:00 2019	④
/dev/ada0p3	2 Mon Jan 10 00:30:00 2019	⑤

- A. (4%) 請說明 full 與 incremental backup 的差異。

Please describe the difference between "full backup" and "incremental backup".

- B. (2%) 若欲取得 Jan 08 的備份，需挑選哪幾份備份檔？（請依序填寫數字）

If we want to retrieve the backup on Jan 08, which backup files are needed? Please answer in numbers with correct order.

- C. (2%) 若欲取得 Jan 10 的備份，需挑選哪幾份備份檔？（請依序填寫數字）

If we want to retrieve the backup on Jan 10, which backup files are needed? Please answer in numbers with correct order.

3. (7%) 以下為 NFS 設定檔 /etc/exports 的內容，試回答以下問題。

The content of /etc/exports is below. Please answer following questions.

```
/usr/src /usr/ports -ro -alldirs -maproot=nobody cs_sa_stu
```

- A. (5%) 請說明此設定所代表的意義為何？請詳細敘述設定檔中每一個部分的含義。（註：cs_sa_stu 並非 hostname）

Please describe the meaning of this configuration. You should explain every part of the configuration. Note that "cs_sa_stu" is NOT a hostname.

- B. (2%) NFS Server 所分享的目錄內可能含有 setuid 程式。為了避免安全性問題發生，在掛載（mount）時可加上哪一參數來停用程式的 setuid 權限？

Files exported by NFS server may contains setuid executables How could we disable setuid permission when mounting external files?

4. (4%) System Service

- A. (2%) 當執行了 telnet www.cs.nctu.edu.tw http，系統會連上 www.cs.nctu.edu.tw 的 port 80，請問系統是根據哪一個系統檔案的設定來得知此對應（http 對應到 port 80）？

When executing "telnet www.cs.nctu.edu.tw http", the system opens connection to port 80 of that host. Please explain which system file describes above mapping (e.g. http maps to port 80).

- B. (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?

5. (15%) 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 implemented the "Name-Based Virtual Hosting" in web servers?

- B. (4%) 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 browsers show "untrusted website" when connecting to a web server that uses 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. (4%) 請問 Apache 的 Name-based Virtual Hosting 功能是否支援 SSL/TLS？為什麼？

Does "Name-based Virtual Hosting" in Apache web server support SSL/TLS? Please explain why or why not.

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. (3%) 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 above question, which technique is suitable for providing web hosting services? Please explain why.

6. (6%) Autofs Replicated Filesystem

A. (2%) 請說明 autofs 提供 replicated filesystem 功能用途為何？

Please describe the functionality of "replicated filesystem" in autofs.

B. (4%) 承上，使用 replicated filesystem 有什麼限制？為什麼？

Continued from above question, what is the main restriction of "replicated filesystem"? Please explain why it has such restriction.

7. (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 above question, why incomplete ARP entries are still recorded instead of being dropped?

8. (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 current kernel, is there any approach to support this device WITHOUT recompiling the kernel?

B. (2%) 承上，重新開機是否仍支援此裝置？為什麼？

Continued from 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 1000，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 1000. 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 above question, how could we keep this configuration working after rebooting without running above command every time?

9. (6%) 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。

Please describe the pros and cons of "microkernel" and "monolithic kernel" respectively. You should focus on "modularization", "optimization" and "size of kernel".

10. (4%) 請解釋以下 PF 規則所代表的涵意是什麼。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 in on fxp0 from { 10.0.0.0/8, !10.1.2.3 }

11. (4%) 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".

12. (4%) 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.

13. (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？

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.

14. (4%) 請說明 Machine Level Virtualization 與 OS Level Virtualization 的不同，以及兩者適合的場景應用：(可舉例說明)

Please explain the difference of "Machine Level Virtualization" and "OS Level Virtualization", and the use scenario of both technology. You may show some examples.