交通大學 計算機網路管理 2020 期末考

NCTU Computer Network Administration Final Exam

Date/Time: 2020/06/18 PM 06:30 ~ 09:00 (2.5 hours)

Open book. Submit your answer in a separate file (TXT/PDF format)

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

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

Short Answer (total 100%, 8 questions)

1. (12%) Postfix 是個被廣泛使用的 Mail Server，其中包含多個 Queue 及程式，試回答下列問題。
   Postfix is a widely used mail server. It contains many queues and sub-programs. Please answer following questions.
   a. (3%) 假設已經在 Postfix 設定了 masquerade_domains 參數，需再設定哪一個參數，才可讓透過該 MTA 轉送出去的信件，其 Header From 以及 Envelope From 都被 masquerade？
      Assumed that a Postfix server is already configured with “masquerade_domains”. Please describe which configuration is needed for applying the masquerading to the “Header From” and “Envelope From”.

   b. (3%) 請分別說明在什麼狀況下信件會被移至 deferred queue 與 hold queue。
      Please explain in which situation that a mail is moved to the “deterred queue”? What about the “hold queue”?

   c. (3)% 試描述 Postfix 設定中，body_checks, header_checks, smtpd_*_restrictions 分別在 SMTP Conversation 中的那一階段發生作用？
      Please describe in which stage(s) of SMTP Conversation that Postfix applies body_checks, header_checks and smtpd_*_restrictions?

   d. (3%) 在 Postfix 中，Restriction Check Results 有 OK, REJECT, DUNNO 三種，請問 OK 與 DUNNO 的差異？
      There are three types of restriction check results in Postfix: OK, REJECT and DUNNO. Please explain the difference between OK and DUNNO.

2. (30%) Anti-Spam 是當今 Mail System 不可或缺的機制，且新型的攻擊型態常透過電子郵件滲透，需持續精進才能有效阻擋各種推陳出新的資安威脅。試回答下列問題。
   Anti-Spam is an indispensable mechanism of the mail systems nowadays. The modern attacking methods usually take the route through email, as a result, it is necessary to improve the anti-spam mechanism to mitigate the various security threats. Please answer the following questions.
   a. (5%) 請說明使用 DNSBL 阻檔 spam 的運作機制，並舉例說明 Mail Server 要如何向 DNSBL 查詢資訊？
      Please describe the mechanism of using DNSBL to block spam, and give an example of how a mail server queries information from a DNSBL.

b. (5%) 請說明 Greylisting 為什麼可以有效減少 spam 的數量，以及為什麼需配合白名單機制，該機制可能的適用情境為何？
Please explain why greylisting can effectively reduce the amount of spam, and why it needs white list mechanism. What is the scenario of using that mechanism?

c. (5%) 請說明 DKIM (DomainKeys Identified Mail) 機制可對郵件提供什麼保證？
Please describe that DKIM (DomainKeys Identified Mail) mechanism can guarantee in the email system.

d. (5%) SPF (Sender Policy Framework) 可用來指定該網域合法的 Outgoing Mail Server。請說明下列 SPF record 所代表的意義為何？
SPF (Sender Policy Framework) can be used to designate the eligible outgroup mail server of a domain. Please explain the meaning of the following SPF record.

```
cs.nctu.edu.tw. 3600    IN  TXT "v=spf1 mx a:mailer.cs.nctu.edu.tw ~all"
```

e. (5%) 假設 cs.nctu.edu.tw 的 MX 和 SPF record 如下。請問 cs.nctu.edu.tw 已經有設定 SPF record 了，為什麼對於這個 domain 的 MX server 也需要各別設定自己的 SPF record 呢？而表中所示 MX 的 SPF record 是否合適？為什麼？
Following are the related MX and SPF records of cs.nctu.edu.tw. Why does the MX server of this domain still need its own SPF record when there is an SPF record for cs.nctu.edu.tw? And is the SPF record of the MX suitable? Why?

```
cs.nctu.edu.tw.          3600    IN  TXT  "v=spf1 redirect=_spf.cs.nctu.edu.tw"
cs.nctu.edu.tw.          3600    IN  MX       10 csmx.cs.nctu.edu.tw.
csmx.cs.nctu.edu.tw.     3600    IN  TXT  "v=spf1 a -all"
```

f. (5%) DMARC (Domain-based Message Authentication, Reporting and Conformance) 可定義網域對於可疑電子郵件的處理方式，無法通過 SPF 或 DKIM 會觸發 DMARC 政策。請說明下列設定所代表的意義為何？
DMARC (Domain-based Message Authentication, Reporting and Conformance) can be used to specify how the receiver handles the specious mails. The mails failed to pass SPF or DKIM will trigger DMARC handlers. Please describe the meaning of the following settings.

```
_dmarc.cs.nctu.edu.tw.  3600    IN  TXT  "v=DMARC1; p=quarantine;
rua=mailto:postmaster@cs.nctu.edu.tw"
```

3. (6%) MX server 處理 SPAM filtering 或是 virus scanning 可能有較高的資源使用，並在處理的信件量大時造成收送延遲的問題。如果做為折衷，我們希望從可以信任的網路來的郵件可以不需要經過過多的檢查，請問該如何設計系統？
MX server processing spam filtering or virus scanning may result in higher resource consumption, and might cause delivery delay when processing large amounts of mails. As a compromise, if we want to let the mail coming from trusted networks skip some checkers, how do we design the mail system?

4. (8%) ICMP 為輔助 TCP/IP 運作的重要協定，其作用可分為 Query 及 Error 兩大類。試回答下列問題。
   ICMP is a supporting protocol in the TCP/IP suite, and can be divided into two categories: Query and Error Reporting. Please answer following questions.
   a. (4%) TCP 會以 TCP RST 來表示 Port Unreachable，而 UDP 則是如何達成此目的？
      TCP responses with TCP RST to represent port unreachable. How does UDP achieve the purpose?

   b. (4%) 為什麼 ICMP Query 類別的訊息通常都會被阻擋？
      Why do ICMP query messages usually be blocked?

5. (6%) NAT 可讓多台終端共用一個 Public IP Address，用來紓緩 IPv4 Address 數量不足，也可利用 NAT 來提供 Server Load Balancing 功能，請簡述該 Translation 功能的運作方式。
   NAT allows multiple devices to share a single public IP address to delay shortages of IPv4 addresses. It also provides the functionality of server load balancing. Please describe how it works to offer load balancing feature using NAT.

6. (10%) LDAP 提供存取、控制及維護目錄資訊，常見的用途為單一登入(Single Sign-On, SSO)。試回答下列問題。
   LDAP is an application protocol for accessing, controlling and maintaining directory information. A common usage of LDAP is to provide single sign-on (SSO).
   a. (5%) 為什麼 Directory ACL 順序很重要，若忽略了順序可能會產生什麼風險？
      Why ordering is important for Directory ACL? What kind of the security risk does the service face if you ignore the ordering of directory ACL configuration?

   b. (5%) 何謂 Overlays？其作用為何？
      What are overlays? What functionality do overlays provide?

7. (20%) SNMP 為當前 TCP/IP 網路廣為使用的網路管理協定，大部份的網管應用皆是以 MIB-II 實作。試回答下列問題。
   SNMP is commonly used in network management for TCP/IP network monitoring. A variety of network management applications are implemented based on MIB-II. Please answer following questions.
   a. (5%) 何謂 MIB (Management Information Base)，其作用為何？
      What is MIB? What functionality does MIB provide?

   b. (5%) SNMP v2c 與 SNMP v3 最大的差異為何？兩者各別的作法為何？
      What is the major difference between SNMP v2c and SNMP v3? What do they do respectively?

   c. (5%) 何謂 SNMP Trap？其應用為何？
      What is SNMP Trap? What is its application?

d. (5%) 若 NMS (Network Management System)與被管理設備(SNMP Agent)間有防火牆阻檔，則防火牆的規則需如何指定才能允許 SNMP 及 SNMP Trap 封包？請說明 TCP/UDP、Port Number 及方向性。
If the firewall is deployed between NMS and managed devices (SNMP Agent), what are firewall rules defined to allow SNMP and SNMP Trap? Please provide TCP/UDP ports and its direction.

8. (8%) 組態管理(Configuration Management)工具可讓軟體安裝、設定佈署、升級等各種作業自動化，利用預先定義的組態設定檔來管理 IT 基礎設施，稱為 IaC (Infrastructure as code)，而組態管理工具百花齊放，請問在評估導入，考量的面向可能有哪些？請至少說明 4 項衡量因子。
Configuration management (CM) tools automate the process of software installation, configuration maintenance, software upgrade, and so on through machine-readable definition files call IaC (Infrastructure as code). What decision criteria do you consider for choosing a suitable CM tool? Please describe at least four factors.