交通大學 計算機網路管理 2020 期中考

NCTU Computer Network Administration Midterm Exam

Date/Time: 2020/04/30 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%, 13 questions)

1. (12%) DHCP 可為網路內的終端裝置配發 IP 位址及相關網路資訊，讓使用者無需手動設定便可存取網路。試回答下列問題。
   The DHCP Server allocates IP addresses and network configuration to devices in the network. This allows clients to connect the network without manual settings. Please answer following questions.

   a. (4%) DHCP 主要提供哪 3 種 IP 配發模式? 請簡述其配發模式。
      There are 3 address allocation mechanisms. Please brief these mechanisms.

   b. (4%) 承上，請分別舉例說明 3 種配發模式可能的應用情境。
      Continued from above question. Please show some examples and scenario for these mechanisms.

   c. (4%) 為什麼 Client 不在收到 DHCP Server 的 DHCP Offer 回應後即使用其所提供的 IP 資訊？
      Why client do not use the IP address just after “DHCP offer”?

2. (12%) Firewall 可根據制定的 Policy 來允許或拒絕封包的進出。試回答下列問題：
   Firewalls will allow or reject packets according to the policy specified. Please answer following questions.

   a. (4%) Stateful 與 Stateless Firewall 在運作上的差異為何？
      What’s the difference between stateful and stateless firewalls?

   b. (4%) Firewall 阻擋封包可 (a) 直接 Drop 且不予回應，也可以 (b) Drop 後給予回應，請說明兩者對 Client 的影響為何？
      There are two ways to block packets (a) just drop it and do not respond (b) drop it and respond the result to the sender. Please brief the behavior of the client according to the two ways.

   c. (4%) Stateful Firewall 可能遭受 TCP half-open 的 DDoS 攻擊，請說明該攻擊如何達成目的。
      Please brief how stateful firewall is attacked by TCP half-open DDoS.

3. (4%) 在 OWASP 2017 的統計報告中，Injection 是資安弱點的第一名，請說明如何有效避免 Injection 攻擊？
   The “injection” is the most vulnerable reason in OWASP 2017. Please describe how to avoid the injection attacks.

4. (4%) 請說明 DMZ 的用途以及所達成的效果，以及簡述會放在 DMZ 內的服務類型為何？
   Please describe why DMZ is designed, and what DMZ does. Please also brief what kind of service will allocated in DMZ.

5. (4%) 請說明三個使用 VPN 的主要原因，以及簡述這些原因的情境。
   Please describe the most 3 important reasons we use VPN, and brief some examples and scenario for the reasons

6. (12%) Load Balancer 可以協助服務擴展以及提升服務可用性。試回答下列問題。
   Load balancers can make the scale of service and improve the availability. Please answer following questions.

   a. (4%) 服務擴展有 2 種方式，請簡述說明作法與優缺點
      Please describe the 2 main methods to scale the service, and their pros and cons.

   b. (4%) 提升服務可用性有 3 種原則，請簡述說明之。
      There are 3 principles for high availability, please describe them.

   c. (4%) 當突發事件造成資源不足，請說明 Graceful Degradation 如何提升當下的服務可用性？
      How does “Graceful Degradation” improve the availability when there is a sudden resource outage?

7. (16%) DNS System & Security
   a. (4%) 請說明何謂 DNS glue record ，並解釋為什麼在 subdomain delegation 時有其必要性。
      Please describe what is DNS glue record, and explain why it is necessary when doing subdomain delegation.

   b. (4%) 為什麼會建議在其他 network 也至少放一個 authoritative DNS server？
      提示：如果重要的 DNS record，如 MX record 查不到的時候會發生什麼事？
      Why is it suggested to put at least one authoritative DNS server in another network?
      Hint: What will happen if some important DNS record, for example, MX record cannot be resolved?

c. (4%) 請解釋 DNSSEC 是如何建立 trust chain。可以從 RRSIG / DS / DNSKEY record 的作用各是什麼還有 server 在設定和 client 在驗證時候如何使用這些 record 說明。
Please explain how DNSSEC establishes the trust chain. It can be started from the functions of RRSIG / DS / DNSKEY record and how to configure these in the server and how clients verify them.

d. (4%) DNSSEC 和 TSIG 有沒有辦法保護「客戶端查了哪些資訊的隱私」的作用？如有請說明如何做到，如無請說明者兩者所提供的安全功能。
Can DNSSEC and TSIG protect the "privacy of what client has queried"? If yes, please explain how they achieve it. If not, please explain what are the secure features they provide.

8. (12%) DNS & Server Load Balancing
   a. (4%) 使用多個 A record 來做 server load balancing 有什麼優點和缺點？
   What are the pros and cons of using multiple A records to do server load balancing?

   b. (4%) 承上題，為什麼不能用多個 CNAME records 來做到？
   Continued from above question. Why is it impossible to be done with multiple CNAME records?

   c. (4%) 承上題，如果用 SRV record 來做 server load balancing 會有什麼限制？
   Continued from above question. What is the limitation of using SRV record to do server load balancing?

9. (4%) 假設預計在一個星期後要進行網頁伺服器 IP 位置更換工作，請問要做哪些準備還有復原工作，讓使用者受到轉換的影響儘量小，並請說明原因？
   If it is planned to do IP address changing of the web server after one week. What are the preparation and recovery tasks to minimize the impact to the users.

10. (8%) 在建立只有內部網路可以使用的服務時，我們還是會設定相關的 DNS record 以方便存取。在設定這種只有內部網路使用的 private domain 時，試回答下列問題。
    When setting up internal service for intranet, we still configure the related DNS records for convenient access. Please answer following questions when setting this kind of private domain which is only used in the intranet.

    a. (4%) Private domain 通常會設定成只有內部網路可以連到的 DNS 可以解析，如果設定成 Internet 上所有 DNS server 都可以解析，加上 DNS record 使用 private IP 或是用 firewall 保護內部的機器，這兩種方法各有什麼優缺點？
    提示：可以從 server 和 client 設定上和使用上的難易度的還有安全的角度分析。
    In most of the cases we configure the private domain can only be resolved by the server which can only be accessed in the intranet. If it is configured to be able to be resolved by all the DNS servers on the Internet, with private IP in the DNS records or using firewall to protect internal hosts, what are the

pros and cons of these two approaches?
Hint: Can be analyzed from the setting and usage at server and client sides, and the security perspective.

b. (4%) 在 domain 的選擇上，通常會使用特定的 subdomain （如 internal.example.com，example.com 為提供公開服務的 domain），如果想要使用自訂的 TLD（如 example.nasa）可不可以做到？如果可以要如何實作？兩種方法各有什麼優缺點？
In most of the cases we use a specific subdomain (e.g. internal.example.com, where example.com is for public service). Is it possible to use a customized TLD (e.g. example.nasa)? If so, how to implement it? What are the pros and cons of these two approaches?

11. (4%) 請說明 e-mail system 中所指的 open relay 意義為何及其可能造成的問題。
Please explain what is “open relay” in the e-mail system. What happens when a mail server becomes an open relay server?

12. (4%) 在 mail envelope 與 mail header 中都有相對應的收件者欄位。請解釋兩者之間的差別。
Both the mail envelope and the mail header have the “receiver” field. Please explain the difference of the two.

13. (4%) 承上題，如果強制要求 mail envelope 與 mail header 的 receiver 欄位必須一致，可能會造成什麼問題？
提示：若不一致的信件會被丟棄，則使用者會受到什麼影響？
Continued from above question, what happens if we enforce the receiver field in the mail envelope and the mail header to be consistent?
Hint: what happens to the users when mails with inconsistent receiver fields are discarded silently?