112 年特種考試地方政府公務人員考試試題

等　別：三等考試
類　科：資訊處理
科　目：資通網路與安全

曹勝老師解題

一、對於 TCP/IP 網路的各項運營管理工作，IP 表頭（IP Header）內各項欄位的識別是很重要的基礎知識，請詳細說明下列 IP Header 欄位的用途：（每小題 4 分，共 20 分）
㈠ Total length
㈡ Identification number
㈢ Fragmentation offset
㈣ Time-to-live
㈤ Protocol

《考題難易》：★★
《解題關鍵》： IP 協定基本題，掌握 IP 表頭內各項欄位即可作答。
《命中特區》：資通網路講義 AF22 P5-22 IP 協定標頭完全命中。

【擬答】：

㈠Total Length：標識整個 IP 數據報文的總長度（Header + Data）。該欄位是 16 位的無號整數，表示以字節為單位的總長度，最大值為 65535 字節。這包括 IP 標頭和 IP 數據（Payload）的總和。

㈡Identification Number：用於標識 IP 分段的唯一性。當 IP 數據報文需要被分段傳輸時，每一個分段都會有相同的標識號，以區分同一數據報文的不同分段。確保在目的地重新組裝時能正確還原原始數據。

㈢Fragmentation Offset：表示分段中的數據相對於原始數據的位置。以 8Bytes 為單位，偏移量指示分段在原始數據中的位置。用於確定分段的正確順序，以便在目的地進行重新組裝。

㈣Time-to-Live (TTL)：表示 IP 數據報文在網路中可以經過的最大節點數（路由器或網關）。TTL 是一個 8 位的欄位，每經過一個節點，TTL 減 1。當 TTL 減為零時，數據報文將被丟棄，同時也避免了在網路中無窮循環的情況。

㈤Protocol：標識 IP 數據報文中的上層協議。該欄位是一個 8 位的欄位，代表了上層協議的種類，例如 TCP（6）、UDP（17）或 ICMP（1）。這使得在目的地能夠確定應該由哪個協議進行處理，並正確解釋數據報文的內容。

二、5G 行動網路日益普及，且除了 5G 公共服務外還提供 5G 企業專用網路。請問：（每小題 10 分，共 20 分）
㈠相較於 4G，5G 行動網路的特點有那些？請詳細說明之。
㈡企業採用 5G 行動專網帶來的安全風險有那些？請條列並說明之。

《考題難易》：★★★
《解題關鍵》： 5G 應用進階題，除需要了解 5G 相對於 4G 的特點外，也要了解 5G 專網始可作答。
《命中特區》：資通網路講義 AF22 P2-37 5G 特點完全命中。

【擬答】：

㈠5G 行動網路的特點相較於 4G：

1. 更高的傳輸速率：5G 提供更高的傳輸速率，理論上可達到數 Gbps 等級，比 4G 快數十倍。這種高速率有助於支持更多的應用，包括高清影片串流、虛擬現實（VR）、擴增現實（AR）等。
2. 低延遲（Ultra-Low Latency）：5G 具有極低的傳輸延遲，通常在毫秒以下，遠低於 4G。

這對實時應用，如遠端醫療、自動駕駛汽車等至關重要。

3. 多連接性（Massive Device Connectivity）：5G 設計用於支援大量同時連接的設備，實現 IoT（物聯網）的應用，從智慧城市到智慧家居等。
4. 更高的頻譜效益：5G 使用的高頻波段提供更寬的頻寬，提高了頻譜效益。這意味著更多的數據能夠在相同的時間內進行傳輸。
5. 網路切片（Network Slicing）：5G 支援網絡切片，使網絡能夠按需配置和調整，以滿足不同應用的需求，例如為企業提供專用的網路。

㈡企業採用 5G 行動專網帶來的安全風險：

1. 物聯網攻擊：大量連接的設備和物聯網終端可能成為攻擊的目標，攻擊者可能利用弱點進行入侵，癱瘓整個網絡。
2. 高頻波段安全性挑戰：5G 使用的高頻波段信號傳播範圍較小，容易受到干擾。這可能增加竊聽和干擾的風險，需要更嚴格的加密和安全機制。
3. 網路切片隔離不足：當企業使用 5G 網絡切片時，不當的配置可能導致不同切片之間的數據共享或干擾，增加機密性和隱私風險。
4. 虛擬化安全性問題：5G 的網絡虛擬化和軟體定義網絡可能受到虛擬網絡功能的漏洞或攻擊，需要強化安全措施。
5. 端到端加密的需求：由於高速率和低延遲的特性，對端到端加密的需求變得更加迫切，以確保敏感信息在整個通信過程中得到保護。

三、DNS（Domain Name Service）是重要的網路服務，請回答下列有關 DNS 問題：

㈠何謂 Zone file？請說明其用途及內容。（5 分）

㈡請說明迭代式 DNS 查詢（iterative DNS query）的工作原理。（10 分）

㈢當 SOC（Security Operation Center）對受管理組織下某台主機發出「DNS Open Resolver 弱點」的告警訊息時，代表後者可能存在的資安危害為何？請說明之。（5 分）

《考題難易》：★★★

《解題關鍵》： DNS 相關進階題，需要理解 DNS 中 Zone file 概念、迭代式 DNS 查詢過程與告警訊息意義始可作答。

《命中特區》：資通網路講義 AF22 P7-4 DNS 相關協定完全命中。

【擬答】：

㈠Zone File：

Zone file 是 DNS 伺服器上的文本文件，用於描述一個特定的 DNS 區域（Domain Zone）的配置信息。每個域名都有一個相應的區域，而其配置信息則存儲在該區域的 Zone file 中。Zone file 的主要用途是指示 DNS 伺服器如何解析域名。它包含了該區域中所有主機的記錄，如主機名稱到 IP 地址的映射，郵件伺服器的信息，以及其他 DNS 記錄類型。Zone file 的典型內容包括：

1. SOA（Start of Authority）記錄： 包含有關區域的基本信息，如域名的管理者、域名的主機名稱、序列號等。
2. NS（Name Server）記錄： 指定該區域的 DNS 伺服器。
3. A（Address）記錄： 將主機名稱映射到 IPv4 地址。
4. AAAA（IPv6 Address）記錄： 將主機名稱映射到 IPv6 地址。
5. MX（Mail Exchange）記錄： 指定郵件伺服器的信息。
6. 其他類型的 DNS 記錄，如 CNAME、PTR 等。

㈡迭代式 DNS 查詢：迭代式 DNS 查詢是一種 DNS 查詢模式，其中 DNS 客戶端向 DNS 伺服器發送查詢請求，如果伺服器無法立即提供準確的答案，它會指示客戶端到其他伺服器進行進一步查詢，直到找到準確的答案或達到查詢的最大次數。其查詢步驟：

1. 客戶端向本地 DNS 伺服器發送查詢。
2. 本地 DNS 伺服器查詢自己的緩存，如果有答案就返回給客戶端。
3. 如果本地 DNS 伺服器緩存中沒有答案，它向根 DNS 伺服器發送查詢。
4. 根 DNS 伺服器指示本地 DNS 伺服器查詢頂級域（TLD）伺服器。

5. TLD 伺服器指示本地 DNS 伺服器查詢次級域伺服器。
6. 此過程繼續，直到找到包含準確答案的權威 DNS 伺服器。
7. 權威 DNS 伺服器返回答案給本地 DNS 伺服器。
8. 本地 DNS 伺服器將答案返回給客戶端，同時將答案存入緩存。

㈢DNS Open Resolver 弱點：具有下列資安危害：

1. 放大攻擊（DNS Amplification Attack）： 開放式 DNS 伺服器容易被攻擊者利用進行放大攻擊。攻擊者向開放式 DNS 伺服器發送小型查詢，伺服器回應較大的應答，攻擊者可以利用這種方式放大攻擊流量，使目標受到超過其預期容量的流量攻擊。
2. 用於反射攻擊： 開放式 DNS 伺服器可能被用作反射攻擊的中繼站，攻擊者可以通過伺服器向目標發送大量的 DNS 查詢，使得目標受到攻擊。
3. DNS 洪水攻擊： 攻擊者可以通過向開放式 DNS 伺服器發送大量無效的 DNS 查詢，使其過載，影響正常的 DNS 服務。

四、零信任架構（Zero Trust Architecture, ZTA）是目前政府大力推動的資訊安全架構：（每小題 10 分，共 20 分）

㈠請詳細說明 ZTA 的概念和推動 ZTA 的動機。

㈡實現 ZTA 的核心機制有那些？請條列並說明之。

《考題難易》：★★
《解題關鍵》：ZTA 概念題，掌握 ZTA 的概念和推動動機、實現核心機制即可作答。
《命中特區》：資通安全講義 AF24 P1-110 112 調查局特考題目完全命中。

【擬答】：

㈠ZTA 的概念和推動動機：

零信任架構 (Zero Trust Architecture, ZTA) 是一種資訊安全架構，其核心理念是不信任任何內部或外部的用戶、系統或服務，始終保持高度警惕，即使是內部網路中的資源也不例外。ZTA 不以網絡位置為基礎進行信任，而是將信任的範疇擴展到每個訪問者、設備、應用程序或資源。其推動動機：

1. **傳統安全模型的不足：** 傳統的安全模型通常基於「防禦內部，信任外部」的理念，但現代威脅環境中，內部威脅和外部威脅都可能對系統造成嚴重威脅。

2. **遠端工作趨勢：** 遠端工作的普及使得員工可以從任何地方訪問企業資源，因此需要一種不依賴於傳統防火牆的安全模型。
3. **數據價值提升：** 數據成為企業最重要的資產之一，需要更嚴格的安全措施來保護數據的完整性和機密性。
4. **先進持續性威脅（APT）：** 對抗先進的攻擊需要更進一步的安全措施，不僅僅是依靠邊界安全。

㈡實現 ZTA 的核心機制：

1. 身分驗證與授權：可用多因素身分驗證 (MFA)**確保使用者身分的真實性，防止未授權訪問。也要嚴格控制每個用戶或系統的權限，僅授予必需的權限。**
2. 微分隔離 (Micro-Segmentation)：運用網絡區段化**劃分網絡為多個區段，限制不同區段間的通信，減小攻擊表面。**
3. 持續身分驗證 (Continuous Authentication)：運用行為分析**監測用戶行為，及時檢測異常活動，並可能需要重新驗證身分。**
4. 安全接入：利用虛擬私人網絡 (VPN)**提供加密通道，確保通信的安全性。進行**零信任網絡存取 (ZTNA)，也就是**基於需求的、有條件的網絡存取，不再依賴傳統的 VPN。**
5. 數據加密：採用端到端加密，**保護敏感數據在傳輸過程中的安全。**
6. 事件監控和反應：採取實時監控**持續監測系統，及時發現異常行為。而後以**自動化威脅應對，**對於檢測到的威脅自動進行應對，減少反應時間。**
7. 安全文化和教育：進行培訓和教育，**向用戶和管理層灌輸零信任的安全意識，提高整體安全文化。**

五、防火牆（Firewall）是當今企業常見的安全防護設備，請問：

㈠企業常用防火牆隔離出一個網段，稱為 DMZ（Demilitarized Zone），請詳細說明其用意為何。（5 分）

㈡ WAF（Web Application Firewall）和傳統的封包過濾式防火牆（Packet filtered Firewall）有何不同？請詳細說明。（10 分）

㈢防火牆常根據從外部收到的 IOC（Indicator of Compromise）來做規則調整，請問 IOC 的意義為何？（5 分）

《考題難易》：★★★
《解題關鍵》：　防火牆應用進階題，了解 DMZ、WAF 與 IOC 的意義即可作答。
《命中特區》：資通安全講義 AF24 P3-16 防火牆說明完全命中。

【擬答】：

㈠**DMZ（Demilitarized Zone）** 是一個位於企業網絡中的區段，處於內部網絡和外部網絡之間，其用意為：

1. 隔離敏感資源： **DMZ 用於隔離內部網絡和外部網絡，將一些對外提供服務的伺服器（如網頁伺服器、郵件伺服器）放置於 DMZ 中，以保護內部網絡的敏感資源。**
2. 提供對外服務： **DMZ 中的伺服器提供對外的服務，例如網站訪問、郵件收發等，這樣外部用戶能夠訪問這些服務而無需直接進入內部網絡。**
3. 加強安全防護： **DMZ 中的伺服器受到額外的安全保護，例如應用特定的防火牆規則，以減少攻擊者對內部網絡的風險。**

㈡WAF（Web Application Firewall）和傳統的封包過濾式防火牆的不同：

1. WAF（Web Application Firewall）：主要保護網站應用層。針對 Web 應用的攻擊，如 SQL 注入、跨站腳本（XSS）等提供保護。通過深度檢測 HTTP 流量，分析應用層的請求和響應。專注於保護網站和 Web 應用。
2. 封包過濾式防火牆（Packet Filtered Firewall）：主要關注通信的封包。依賴於封包的源、目的、協定和端口等信息進行過濾。根據封包的基本屬性進行過濾，通常處於網絡的邊界。更廣泛應用於整個網絡，不僅限於 Web 應用。

㈢IOC（Indicator of Compromise）

是指可能表明系統或網絡受到威脅的特定跡象或特徵。IOC 的意義在於：

1. **偵測威脅：** IOC 用於檢測可能的安全事件，例如異常行為、惡意文件、攻擊模式等，有助於發現是否有系統受到威脅。
2. **識別攻擊：** 通過識別 IOC，安全專業人員能夠識別可能的攻擊活動，包括惡意軟件、命令和控制伺服器等。
3. **改進安全防禦：** 使用 IOC 的信息能夠改進安全防禦機制，更新防火牆規則、入侵檢測系統等，以增強對已知威脅的防禦能力。