111 年公務人員高等考試三級考試試題

類　　科：資訊處理
科　　目：資通網路與安全

一、關於 TCP/IP 協定,請問：

㈠ TCP (Transmission Control Protocol) 和 UDP (User Datagram Protocol)都位於傳輸層，請說明這兩個協定各自有何特色?(10 分)

㈡請詳細說明何謂 TCP 三方握手(3-way handshaking)協定?(5 分)

㈢為何 TCP 三方握手協定會造成癱瘓服務(Denial of Service)攻擊?(5 分)

1.《考題難易》：★★
*2.《解題關鍵》：**TCP 協定基本題，掌握 TCP 與 UDP 協定概念，搭配 TCP 中三方握手協定與弱點即可完美作答。***
*3.《命中特區》：**F1A22 資通網路講義 P545 命中㈠，H1K21 資通安全講義 P232 命中㈡㈢***

【擬答】：

㈠ TCP 定義了一個可靠資料流服務的協定，可以在一個不可靠互連的網路上提供可靠點對點的位元組流，支援連結管理、流量控制、錯誤控制、壅塞控制等傳輸層功能。與 UDP 通訊協定作功能比較如下表：

協定 / 分類	TCP	UDP
連接導向	連接導向，運用三方握手(3-way handshaking)協定以建立與斷開連結	無連接導向
可靠傳輸	支援可靠傳輸	不可靠傳輸
流量控制	支援信用方案流量控制	不支援
錯誤控制	檢查標頭、資料與概念性虛擬標頭，採用 checksum	採用檢查和
壅塞控制	支援	不支援
採用之應用程式	FTP	TFTP
採用理由	要求可靠傳送	強調傳輸速度

㈡ TCP 採用三方握手(3-way handshaking)協定以建立與斷開連結，當使用者要跟目標主機通訊時，會先送出一個 SYN 封包來要求目標主機進行通訊，目標主機收到後會回應一個 SYN-ACK 封包給使用者，使用者再送一個 ACK 封包給目標主機確認。然後才開始進行通訊。

㈢這是利用三向交握的弱點，進行請求氾濫攻擊(SYN Flooding Attack)，惡意地送出許多 TCP SYN 封包，使得目標主機以為要進行通訊，便開啟一個通訊埠並傳送 SYN-ACK 訊息給使用者，並等待使用者回覆 ACK 封包，這個等待必須等到該封包溢時(Overflow)才會移除，若一個時段內有多個這樣的等待事件，會使得系統處理速度變緩慢。

二、交換器(Switch)和路由器(Router)是現代公司常見的網路設備，請回答下列問題：

㈠請從用途及特性詳細說明這兩種設備的區別。(15 分)

㈡ RSTP(Rapid Spanning Tree Protocol)是用在交換器還是路由器上的協定?回答時需說明正確的理由才予以計分。(5 分)

1.《考題難易》：★★★
*2.《解題關鍵》：**網路連結設備基本題，掌握交換器和路由器概念，搭配 106 司法特考、調查局特考類似題即可完美作答。***
*3.《命中特區》：**F1A22 資通網路講義 P4~5 命中㈠， P329~331 命中㈡***

【擬答】：

㈠交換器和路由器用途及特性區別：

1. 交換器分為第二層交換器（layer-2 switch）與第三層交換器（layer-3 switch）。第二層交換器在區域網路通訊傳輸中僅以第二層（資料鏈結層）的資訊來作為交換之依據，通常此類交換器先以學習的方式，針對其上每一個 port 記錄該區段的 MAC Address，再根據第二層 frame 中的目的地位址傳送該 frmae 至目的地的 port（或區段），其他 port（或區段）將不會收到該 frame。由於只判斷第二層的資訊故其處理效能佳，且其有效隔絕區段間非往來 frame，提昇網路的傳輸效能，但是 Layer 2 的 Switch 並無法有效的阻絕廣播領域及 NetBEUI 協定的廣播封包，易造成廣播風暴問題。㈡第三層交換器（layer-3 switch）又稱為 IP Switch 或 Switch Router,工作於第三層（網路層），藉由解析第三層資訊將封包傳到目的地。有別於傳統的路由器以軟體的方式來執行路由運算與傳送，Layer 3 Switch 是以硬體的方式（通常由專屬 ASIC 來進行）來加速路由運算與封包傳送。Layer 3 Switch 的每一個連接埠（port）都是一個子網路（Subnet），而一個子網路就單獨是一個廣播領域（Broadcast Domain），因此每一個 port 的廣播封包並不會流竄到另一個 port。

2. 路由器（Router）

這是在 OSI 協定中的網路層負責轉送分封的裝置，與 bridge 類似，但是此一裝置在網路層工作，因此其所連接的兩個網路可能在網路層採用不同的協定，其主要功能為分封路徑選擇。

㈡生成樹協定（Spanning Tree Protocol，STP），是一個作用在 OSI 網路模型中第二層的通信協定。基本應用是防止交換機冗餘鏈路產生的迴圈，用於確保乙太網路中無迴圈的邏輯拓撲結構，從而避免廣播風暴大量占用交換機的資源。RSTP 是一種能夠加快這種收斂過程的協定，算是 STP 的加強版本，能更快的收斂網路，將循環網路修剪成無循環的樹狀網路，從而避免包在循環網路中的增生和無限循環。因此 RSTP 是用在交換器上的協定。

三、NAT(Network Address Translation)是許多現代網路設備內建的功能，請問：

㈠ NAT 的功用及原理為何?又使用 NAT 有何缺點?請說明之。(15 分)

㈡許多公司使用 NAT 的目的是降低網路遭受攻擊的風險，請說明其理由。(5 分)

1.《考題難易》：★★
*2.《解題關鍵》： **NAT 基本題，掌握 NAT 協定概念即可作答。***
*3.《命中特區》：**F1A22 資通網路講義 P373 完全命中***

【擬答】：

㈠**網路位址轉換**（Network Address Translation， NAT）是一種在 IP 封包通過路由器或防火牆時重寫來源 IP 地址或目的 IP 位址的技術。這種技術被普遍使用在有多台主機但只通過一個公有 IP 位址存取網際網路的私有網路中。利用 NAT 協定進行網路位址轉譯，允許在 RFC1981 標準中定義的私人專有使用的 IP 位址，這段位址可作為企業或單位內部自行運用的 IP 位址，而無須經過申請的手續。當資訊由本地網路向網際網路傳遞時，傳送端位址從專有位址轉換為公用位址。由路由器跟蹤每個連接上的基本資料，主要是目的端位址和埠。當有回覆返迴路由器時，它通過輸出階段記錄的連接跟蹤資料來決定該轉發給內部網路的哪個主機；如果有多個公用位址可用，當封包返回時，TCP 或 UDP 客戶機的埠號可以用來分解封包。對於網際網路上的通信，路由器本身充當傳送端和目的端。NAT 的缺點：

1. NAT 主機並沒有建立真正的 IP 位址，並且不能參與一些網際網路協定：例如一些需要初始化從外部網路建立的 TCP 連接和無狀態協定（比如 UDP）無法實現。除非 NAT 路由器管理者預先設定了規則，否則送來的封包將不能到達正確的目的位址。一些協定有時可以在應用層閘道器（見下）的輔助下，在參與 NAT 的主機之間容納一個 NAT 的實例，比如 FTP。NAT 也會使安全協定變得複雜，比如 IPsec。
2. 端對端連接是被 IAB 委員會（Internet Architecture Board）支援的核心網際網路協定之一，因此有些人據此認為 NAT 是對公用網際網路的一個破壞。

㈡ NAT 除了帶來方便和代價之外，對全雙工連接支援的缺少在一些情況下可以看作是一個有好處的特徵而不是一個限制。在一定程度上，NAT 依賴於本地網路上的一台機器來初始化和路由器另一邊的主機的任何連接，它可以阻止外部網路上的主機的惡意活動。這樣就可以阻止網路蠕蟲病毒來提高本地系統的可靠性，阻擋惡意瀏覽來提高本地系統的私密性。很多具有 NAT 功能的防火牆都是使用這種功能來提供核心保護的。

四、在網路駭客行為難以完全禁絕的情況下，現代企業需採用各種網路安全設備來提供防護，其中入侵偵測系統(IDS)和防火牆(Firewall)就是常見設備，請問：

㈠入侵偵測系統和防火牆在功能上和部署位置上有何區別?請詳細說明之。(15 分)

㈡入侵偵測系統可以分為主機型以及網路型，請說明這兩種類型的差別。(5 分)

1.《考題難易》：★★
2.《解題關鍵》：網路與通訊安全基本題，掌握防火牆、IDS 概念，即可作答。
3.《命中特區》：H1K21 資通安全講義 P220~221(防火牆)、P225~226(IDS)完全命中

【擬答】：

㈠入侵偵測系統和防火牆在功能上和部署位置的區別

1. 防火牆（Firewall）是一個架設在網際網路與內網之間的資安系統，根據持有者預定的策略來監控往來的傳輸。防火牆可能是一台專屬的網路裝置，也可執行於主機之上，以檢查各個網路介面的網路傳輸。它是目前最重要的一種網路防護裝置，從專業角度來說，防火牆是位於兩個或以上網路間，實行網路間存取或控制的一組元件集合之硬體或軟體。

2. 入侵檢測系統（Intrusion-detection system，IDS）是一種網路安全裝置或應用軟體，可以監控網路傳輸或者系統，檢查是否有可疑活動或者違反企業的政策。偵測到時發出警報或者採取主動反應措施。它與其他網路安全裝置的不同之處便在於，IDS 是一種積極主動的安全防護技術。

3. IDS 不同於使用一系列靜態規則來放行網路連接的傳統防火牆(區別於下一代防火牆)。本質上，為避免網路上的入侵，防火牆會限制網路間的存取，不關注網路內部的攻擊。IDS 也能監視來自系統之內的攻擊。傳統上，這是通過對網路通信進行檢驗，而實現對常見攻擊模式的鑑定並行出警告。

㈡主機型 IDS 及網路型 IDS 的差別

1. 主機入侵檢測(Host IDS,HIDS)：安裝於被保護的主機中，主要分析主機內部活動，包括系統日誌、系統調用、檔完整性檢查，並佔用一定的系統資源。主要靠紀錄或知識庫來分析主機上的各種行為，進而判斷是否有異常行為發生。這類型架構的缺點是每部主機都需安裝一套個別的入侵偵測系統，且這些入侵偵測系統多半與主機的作業系統相關，因此不同的作業系統間入侵偵測系統多半不能交互作用。
2. 網路入侵檢測(Network IDS, NIDS)：安裝在被保護的網段中，採用混雜模式監聽分析網段中所有的資料包，亦可即時檢測和回應，具有作業系統無關性，也不會增加網路中主機的負載。

五、在網路運作中，代理伺服器(Proxy server)常扮演重要角色，請回答下列問題：(每小題 10 分，共 20 分)

㈠代理伺服器的功用及運作原理為何?請說明之。

㈡何謂反向代理伺服器(Reverse proxy server)?請說明其功用及運作原理。

1.《考題難易》：★★★
2.《解題關鍵》：**代理伺服器概念題，掌握代理伺服器與反向代理伺服器概念，即可完美作答。**
3.《命中特區》：**H1K21 資通安全講義 P224 命中代理伺服器，反向代理伺服器可由資訊隱藏推得。**

【擬答】：

㈠代理(Proxy)是一種特殊的網路服務，允許一個終端（一般為客戶端）通過這個服務與另一個終端（一般為伺服器）進行非直接的連接。一些閘道器、路由器等網路裝置具備網路代理功能。一般認為代理服務有利於保障網路終端的隱私或安全，在一定程度上能夠阻止網路攻擊。提供代理服務的電腦系統或其它類型的網路終端稱為代理伺服器(Proxy Server。一個完整的代理請求過程為：客戶端首先根據代理伺服器所使用的**代理協定**，與代理伺服器建立連接，接著按照協定請求對目標伺服器建立連接、或者獲得目標伺服器的指定資源（如：檔案）。在後一種情況中，代理伺服器可能對目標伺服器的資源下載至本地快取，如果客戶端所要取得的資源在代理伺服器的快取之中，則代理伺服器並不會向目標伺服器傳送請求，而是直接傳回已快取的資源。一些代理協定允許代理伺服器改變客戶端的原始請求、目標伺服器的原始回應，以滿足代理協定的需要。

㈡反向代理伺服器是代理伺服器的一種。伺服器根據客戶端的請求，從其關聯的一組或多組後端伺服器（如 Web 伺服器）上取得資源，然後再將這些資源返回給客戶端，客戶端只會得知反向代理的 IP 位址，而不知道在代理伺服器後面的伺服器叢集的存在。與前向代理不同，前向代理作為客戶端的代理，將從網際網路上取得的資源返回給一個或多個的客戶端，伺服器端（如 Web 伺服器）只知道代理的 IP 位址而不知道客戶端的 IP 位址；而反向代理是作為伺服器端（如 Web 伺服器）的代理使用，而不是客戶端。客戶端藉由前向代理可以間接存取很多不同網際網路伺服器（叢集）的資源，而反向代理是供很多客戶端都通過它間接存取不同後端伺服器上的資源，而不需要知道這些後端伺服器的存在，而以為所有資源都來自於這個反向代理伺服器。