110 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

曹勝老師解題

一、近年來員工在家工作的需求量日益增加，因此企業建置 VPN，提供員工遠端登錄企業網路。請說明 VPN 所採用的 IPSEC 運作原理，以及如何管理 VPN 避免企業遭受攻擊。(25 分)

1.《考題難易》：★★
2.《解題關鍵》： VPN/IPsec 基本題，掌握 IPsec 協定概念，搭配 106 國安特考、108 高考類似題即可完美作答。
3.《命中特區》：資通網路講義 P608、P688 頁完全命中

【擬答】：

㈠IPsec 被設計用來提供 1.入口對入口通信安全，由單個節點提供分組通信的安全性給多台機器（甚至可以是整個區域網路）；2.端到端分組通信安全，由作為端點的電腦完成安全操作。並經由此二模式以構建虛擬私人網路（VPN）。IPSec 應用情境如下：

1.傳輸模式（Transport mode）：僅加密或認證上層協定的資料，例如在區域網路中的兩台電腦 A 與 B，可直接建立連線（不必經由路由器或防火牆），且 A 與 B 具有處理 IPSec 封包的能力時，則可使用 IPSec 的傳輸模式。

2.通道模式（Tunnel mode）：IPSec 會加密或認證整個封包，並在最外面再加上一個新的 IP 表頭，當 IPSec 連線兩端的電腦有一端或兩端不具處理 IPSec 封包能力，而必須透過具有 IPSec 能力的路由器或防火牆來代為處理 IPSec 封包時，即必須使用通道模式。

㈡在 VPN 網路上，都希望將內部的網路位址隱藏起來，並透過 NAT（Network Address Translator）將內部位址轉換到外部位址，區域網路透過 Internet 網路做 VPN 連接，並且將 IPSec AH Tunnel 與 NAT 軟體安裝於雙方網路的『安全閘門』（Security Gateway, SG）上，當內部網路 A 的工作站欲傳送封包給內部網路 B 的工作站時，SG-A 將工作站 A 所發送的封包經由 IPSec AH Tunnel 包裝。區域網路 B 的 SG-B 收到封包後，再拆解外部標頭，並從事認證的工作，如果認證無誤的話，便捨棄外部標頭，恢復原來封包格式，並發送到內部網路；工作站 B 再由網路上收到該封包。如此，對雙方工作站而言，並不知道有 VPN 網路的存在，猶如在同一區域網路上運作一樣。

二、DNS 通訊協定並不安全，因此 IETF 提出 DNSSEC 期望改善其安全問題。請說明 DNSSEC 運作原理、所提供之安全服務、可防禦之攻擊以及無法防禦之攻擊。(25 分)

1.《考題難易》：★★★
2.《解題關鍵》：DNSSEC 應用題，需要掌握 DNS 運作方式，搭配 103 調查局特考資訊安全實務科目類似題可以完美作答。
3.《命中特區》：資管與資通安全講義 P573 完全命中

【擬答】：

㈠域名系統安全擴充（Domain Name System Security Extensions， DNSSEC）是 IETF 對確保由域名系統（DNS）中提供的關於網際網路協定（IP）網路使用特定類型的資訊規格套件。它是對 DNS 提供給 DNS 客戶端（解析器）的 DNS 資料來源進行認證，並驗證不存在性和校驗資料完整性驗證，但不提供機密性和可用性。

㈡DNSSEC 旨在保護應用程式（以及服務這些應用程式的快取解析器）免受偽造或不當操縱的 DNS 數據所造成的影響（例如域名伺服器快取污染的數據）。來自 DNSSEC 保護區的所有答案都經過數位簽章。通過檢驗數位簽章，DNS 解析器可以核查資訊是否與區域所有者發布的資訊相同（未修改和完整），並確係實際負責的 DNS 伺服器所提供。雖然保護 IP 位址的正確性是許多使用者關注 DNSSEC 的直接課題，DNSSEC 還可以保護 DNS 中發

布的其他任何數據：包括文字記錄（TXT）和郵件交換記錄（MX），並可用於引導發布參照儲存在 DNS 中的加密憑證的其他安全系統：例如憑證記錄（CERT 記錄，RFC 4398），SSH 指紋（SSHFP，RFC 4255），IPSec 公鑰（IPSECKEY，RFC 4025）和 TLS 信任錨（TLSA，RFC 6698）。

㈢DNSSEC 可防禦之攻擊

1. 資料完整性 (data integrity)

DNSSEC 使用數位簽章的技術，將每筆 RR 做簽章產生 RRSIG (Resource Record Signature)，而收到資料方可使用 Public Key + RRSIG 來驗證是否為原本詢問之 RR 紀錄，以此來驗證中間是否有被竄改。

2. 來源可驗證性 (origin authentication of DNS data)

在 DNSSEC 中，所謂的公正的第三方就是上層的 Domain DNS Server，也就是 DNS Server 必須將自己的 Public Key (DNSKEY) 做一次數位簽章後放在 Parent Zone Server，這種新的 RR(Resource Record) types 稱為 DS(Delegation Signer)，因此由 Parent Zone 中的 DS 紀錄可驗證 Child Zone 之 DNSKEY 確實是正確且未經竄改。

3. 可驗證之不存在性 (authenticated denial of existence)

將所有 DNS 紀錄依照字母排序，而在每個網址間加上一筆 NSEC 紀錄並做電子簽章。當查詢到不存在的網址時，DNSSEC 會回應 NSEC 紀錄，查詢者可比對 NSEC 紀錄中前後對應的字母來確認是否真的不存在，這就是所謂的"可驗證之不存在性"。

㈣DNSSEC 無法防禦之攻擊：

1. 隱密性(Confidentiality)

DNSSEC 傳遞的 RR & 及 RRSIG 傳輸過程皆未加密，因此中間可能被 sniffer 之設備或程式讀取。但被讀取不代表能假造，因為駭客並無 DNS Server 之 Private Key，因此無法假造出 RRSIG 的資料而不被發覺。

2. 服務可用性(Availability)

DNSSEC 僅是一項服務，若有駭客發動 DDoS 攻擊，不斷的詢問成千上萬個網址，則 DNS Server 可能因負荷過重而無法正常運作。不過這項弱點應是所有 Internet 服務皆共有的現象，而不單是 DNSSEC 之弱點。

三、分散式阻斷服務(Distributed Denil of Servce，簡稱 DDoS)攻擊可能造成網路無法使用，因此網管人員需採取一些防範措施，避免網路運作異常。DDoS 攻擊可分為三大類:流量為基礎之攻擊、通訊協定攻擊以及 Layer 7 DDoS 攻擊。若某網站伺服器被 Layer 7 DDoS 攻擊，請舉例說明 Layer 7 DDoS 攻擊，以及防禦方式。(25 分)

1.《考題難易》：★★★
2.《解題關鍵》：DDoS 進階應用題，掌握 DDoS 概念，配合 110 關務特考類似題即可作答。
3.《命中特區》：資通網路講義 P611-612 DDoS 攻擊與防禦方式完全命中

【擬答】：

㈠分散式阻斷服務(Distributed Denial of Service,簡稱 DDOS)攻擊是各種類型的攻擊，可以集中在一個特定的層。第 7 層攻擊專注於第 7 層功能，如 HTTP，SNMP，FTP 等。第 7 層攻擊需要比網絡層攻擊更少的帶寬和數據包來中斷服務。例如，像 SYN Flood 這樣的網絡層攻擊需要大量數據包來執行有效的 DDoS 攻擊。相反，數量有限的數據包可以大規模地進行 DDoS 攻擊。 Layer7 DDoS 攻擊方式如：

1. HTTP Flood
是應用層 DDoS 攻擊中最突出的。當 HTTP 請求發送到服務器時，它會使用相當多的資源。因此，有限數量的這些數據包能夠利用所有的服務器資源。是以大量消耗系統資源為目的，通過向 IIS 這樣的網路服務程式提出無節制的資源申請來破壞正常的網路服務。旨在透過使 HTTP 伺服器無法處理請求來摧毀 HTTP 伺服器。如果伺服器受到數量超出其處理能力的請求轟炸，該伺服器會丟棄合法的請求，甚至會崩潰。

2. CC(Challenge Collapsar)攻擊是指攻擊者借助代理伺服器類比真實使用者，不斷向目標網站發送大量請求，如頻繁請求某個動態 URL 或某個不存在的 URL，致使源站大量回源，耗盡網站伺服器性能，進而致使目標網站拒絕服務。

3. POST Flood 攻擊
攻擊者利用攻擊工具或者操縱僵屍主機，向目標伺服器發起大量的 HTTP POST 報文，消耗伺服器資源，使伺服器無法回應正常請求。

㈡防禦方式：

1. 威脅情報庫

通過大資料分析平臺，即時匯總分析攻擊事件的日誌，提取攻擊特徵（如 IP、URL、User-Agent、Refer 等），並對這些特徵進行威脅等級評估，形成威脅情報庫，對於高風險性的 IP、UA、URL、Refer 等會自動下發到全網防護節點中，一旦後續請求命中威脅情報庫中的高風險性特徵，則直接攔截，最大限度地提高防禦效率，避免 CC 攻擊對網站的影響。

2. 個性化策略配置：

如請求沒有命中威脅情報庫中的高風險特徵，則通過個性化策略配置（如 IP 黑白名單、IP 訪問頻率控制）防禦攻擊；

3. 日誌自學習：

即時動態學習客戶網站的訪問特徵（如客戶每個資源的訪問量、行為特徵等），建立網站的正常訪問基線，一旦超過基線即進行阻擋。

四、HTTP 乃應用層通訊協定，但未提供資料安全性。前網站多採用 HTTPS 以保護資料安全性。請說明 HTTPS 之運作原理，以及可提供之安全服務。(25 分)

1.《考題難易》：★★
2.《解題關鍵》：本題為 HTTPS/TLS 基本題，掌握 SSL/TLS 協定概念，參考 104 身障特考、110 國安特考類似題即可得解。
3.《命中特區》：資通網路講義 P576-577、P676 完全命中

【擬答】：

㈠超文本傳輸安全協定（HyperText Transfer Protocol Secure， HTTPS）是一種透過計算機網路進行安全通訊的傳輸協定。HTTPS 經由 HTTP 進行通訊，但利用 SSL/TLS 來加密封包。傳輸層安全性協定（Transport Layer Security， TLS）及其前身安全通訊協定（Secure Sockets Layer， SSL）是一種安全協定，目的是為網際網路通訊提供安全及資料完整性保障。

㈡HTTPS 中的 TLS 使用 X.509 認證，之後利用非對稱加密演算來對通訊方做身分認證，之後交換對稱金鑰作為會談金鑰（Session key）。這個會談金鑰是用來將通訊兩方交換的資料做加密，保證兩個應用間通訊的保密性和可靠性，使客戶與伺服器應用之間的通訊不被攻擊者竊聽。