iPAS資訊安全工程師
資訊安全技術概論

iPAS資安證照討論區

私有網路位置 (Private IP)

10.0.0.0/8，10.0.0.0 到 10.255.255.255。

172.16.0.0/12，172.16.0.0 到 172.31.255.255。

192.168.0.0/16，192.168.0.0 到 192.168.255.255。

常見網路設備對應OSI參考模型：

應用層(Application Layer)：代理伺服器(Proxy)、網頁應用防火牆(WAF)，具有檢查和處理應用層資料(例如HTTP請求)的能力。

傳輸層(Transport Layer)：防火牆(Firewall)，傳統防火牆，主要根據IP地址和連接埠(Port)進行資料過濾，實施存取控制。

網路層(Network Layer)：路由器(Router)，依據IP地址決定封包的最佳傳送路徑，實現網際網路間的資料傳輸。

資料鏈結層(Data-Link Layer)：橋接器(Bridge)、交換機(Switch)，透過MAC位址在區域網路內轉發資料。

實體層(Physical Layer)：中繼器(Repeater)、集線器(Hub)，負責訊號的轉發與放大，以擴展網路的覆蓋範圍。

常見通訊協定對應OSI參考模型:

應用層(Application Layer):
DNS(網域名稱系統):網域名稱轉換成IP。DHCP(動態主機設定協定):裝置連上網路自動拿取IP位置。FTP(檔案傳輸協定):傳輸資料使用。SMTP(簡單郵件傳輸協定):寄信使用。HTTP(超文本傳輸協定):瀏覽器上網使用。

傳輸層(Transport Layer):
TCP(傳輸控制協定):傳輸前先建立連線，提供一種可靠的連接導向方式。
UDP(使用者資料報協定):傳輸前不先建立連線，可靠度較低。

網路層(Network Layer):
IP(網際網路協定):負責對封包進行路由和定址。
ICMP(網際網路控制訊息協定):用於傳送控制訊息，例如使用PING指令查看對方主機是否存活。
IPSEC(網際網路安全協定):透過對IP協定的封包進行加密和認證來保護IP協定。

資料鏈結層(Data-Link Layer):
ARP(位址解析協定):IP查詢MAC地址，區域網路實際傳輸使用。

常見通訊協定對應TCP/IP參考模型:

應用層(Application Layer):
DNS(網域名稱系統):網域名稱轉換成IP。DHCP(動態主機設定協定):裝置連上網路自動拿取IP位置。FTP(檔案傳輸協定):傳輸資料使用。SMTP(簡單郵件傳輸協定):寄信使用。HTTP(超文本傳輸協定):瀏覽器上網使用。

傳輸層(Transport Layer):
TCP(傳輸控制協定):傳輸前先建立連線，提供一種可靠的連接導向方式。

UDP(使用者資料報協定) :傳輸前不先建立連線，可靠度較低。

網路層(Network Layer):
IP(網際網路協定):負責對封包進行路由和定址。

ICMP(網際網路控制訊息協定):用於傳送控制訊息，例如使用PING指令查看對方主機是否存活。

鏈結層(Link Layer):
ARP(位址解析協定):IP查詢MAC地址，區域網路實際傳輸使用。

DDOS對應攻擊與OSI層級對應
(感謝資安聊天室肯伊提供)

DDos 攻擊類型與對應 OSI 層級整理		
OSI 層級	DDos 攻擊類型	
Application layer 7	CC attack（CC 攻擊）	消耗資源
	Slow attacks（慢速攻擊）	
	HTTP Flood	
	DNS 洪水攻擊(DNS NXDOMAIN Flood)	佔滿頻寬
Presentation layer 6	TLS 層攻擊(不完整 TLS 會話)	
Session layer 5		
Transport layer 4	Ack Flood	消耗資源
	Land Attack	
	SYN Flood Attack	
	UDP Flood Attack/ Fraggle Attack	佔滿頻寬
Network layer 3	Smurf Attack(ICMP)	佔滿頻寬
	ICMP Flood Attack	
	Ping of Death(ICMP)	
Data link layer 2		
Physical layer 1		

第二層還有MAC Flooding Attack

常見的應用層加密協定(通常有加密最後一碼是S)

- SSH
- TLS
- HTTPS
- SFTP
- SMTPS

常見的應用層沒有加密協定

- Telnet
- SMTP
- HTTP
- FTP

常見的Port

- 微軟網路芳鄰：UDP 137、138和TCP 139、445
- HTTP：TCP 80　　HTTPS：TCP 443
- NTP：UDP 123
- FTP：TCP 21 連線控制，TCP 20 資料傳輸
- SFTP/SSH：TCP 22
- Telnet：TCP 23
- SMTP：TCP 25
- DNS：UDP 53，Zone Transfer使用TCP 53
- POP3：TCP 110　　POP3S 995
- IMAP：TCP 143　　IMAPS 993
- SNMP：UDP 161 162
- LDAP：TCP 389
- SYSLOG：UDP 514
- SQL Server：TCP 1433
- PPTP：TCP 1723
- RADIUS：UDP 1812 1813
- RDP：TCP 3389

14.【題組 2背景描述如附圖】該管理人員安裝網路封包側錄器後，對該 SQL Server持續側錄了一整晚的網路封包，隔天進公司針對所側錄下來的網路封包進行分析，發現在網路封包內容顯示了有一個來自210.34.17.8的 IP位址 在深夜的時候連接至 公司內部該 資料庫主機 TCP 3389埠以及 TCP 1433埠）。請問下列敘述何者較為適當？(112-1規劃)

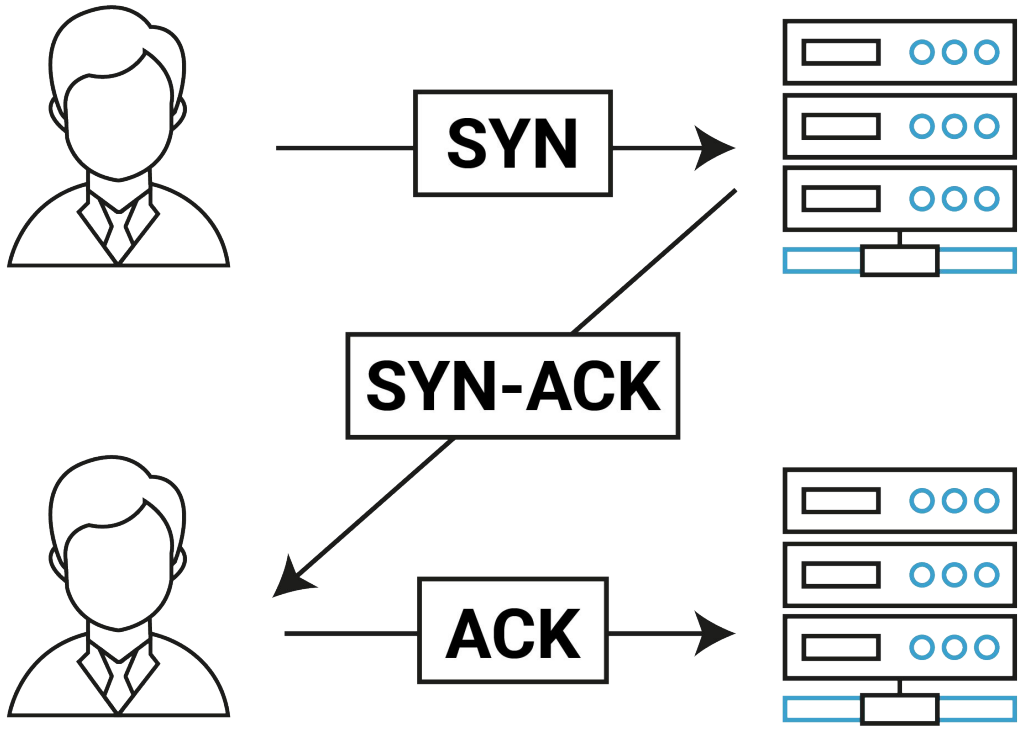
(A) 外部人員使用 VNC軟體進行連線

(B) 外部人員使用虛擬私有網路（ Virtual Private Network, VPN）連接內部網路

(C) 外部人員使用虛擬私有網路（ Virtual Private Network, VPN）連接 SQL Server

(D) 外部人員使用 Remote Desktop Protocol RDP）連接內部網路設備

TCP三項交握協定



techopedia

IPSec協議

協議	認證表頭 AH（Authentication Header）	資料封裝加密 ESP（Encapsulating Security Payload）
提供的保護	身份驗證(IKE)和完整性，避免重送攻擊(replay attack)	身份驗證(IKE)、完整性和機密性
資料流量	增加驗證資訊，不加密資料	加密資料
資料流量	不加密資料，只增加驗證資訊	加密資料，增加額外的 ESP 頭和尾部

IPSec特性

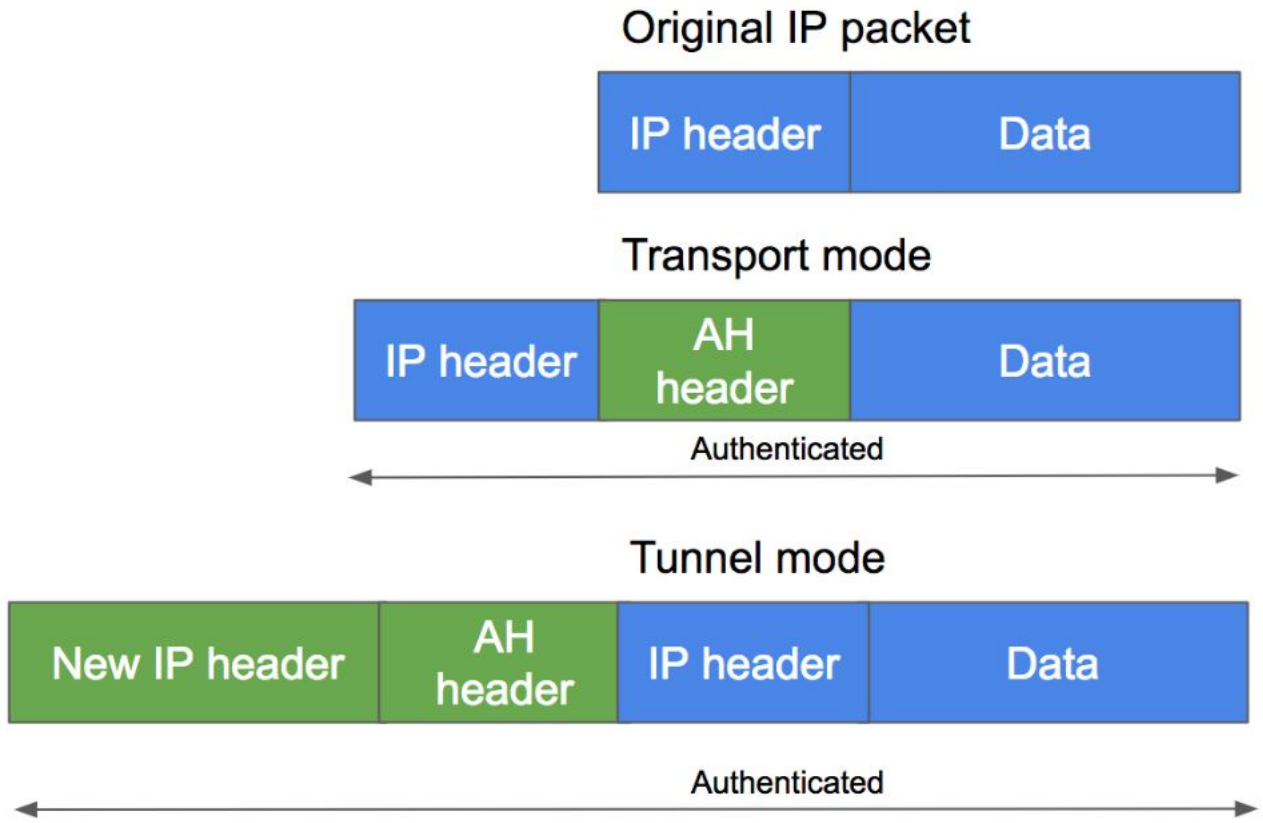
特性	傳輸模式 (Transport Mode)	隧道模式 (Tunnel Mode)
加密範圍	只對資料加密保護	加密整個封包(包含標頭和資料)
標頭處理	保持標頭不變，不加密	添加新的標頭，將原始封包封裝並加密
適用場景	主機之間的點對點通訊，，因不能隱藏主機的IP位置，常用在區域內網的主機通訊	網路閘道間的通信安全，例如總公司和分公司的加密連線，用以取代傳統專線

SSL VPN 和 Site-to-Site VPN 比較

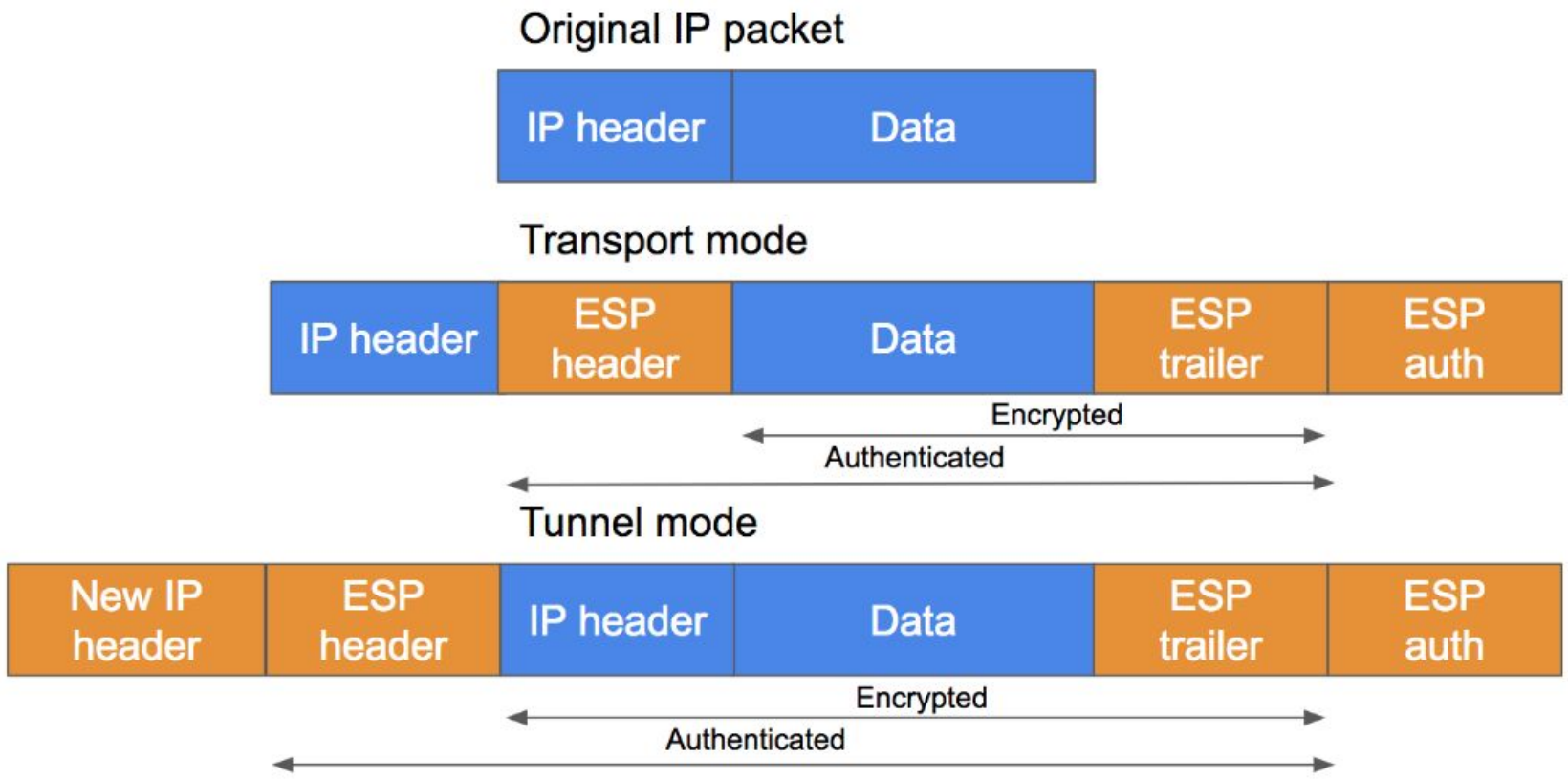
	SSL VPN	Site to Site VPN
例子	學生使用SSL VPN軟體從任何地點連回學校，以取得學校的IP並使用學術網路資源	總公司的網路透過Site to Site VPN和分公司的網路建立一個虛擬通道，彷彿是透過專線連接
加密連線	使用SSL或TLS協議進行加密通訊	通常使用IPsec協議進行加密通訊
OSI層級	主要應用在應用層，但加密本身在傳輸層實現	主要工作在網路層
客戶端需求	可能需要安裝專用軟體，或者可以直接透過網頁瀏覽器訪問	網路閘道間通常需要設定Site to Site VPN連線，用戶端不需要額外設定

SSL VPN 連線成功後
可以取的 140.115 的中央大學 IP

資料來源
(https://kkc.github.io/2018/03/21/IPSEC-note/)



資料來源
(https://kkc.github.io/2018/03/21/IPSEC-note/)



Liunx常見檔案用途

- /etc/shadow：儲存使用者密碼的Hash值。
- /etc/passwd：用戶帳號的基本訊息，但因為必須對所有人可讀，所以將密碼的Hash值放到只有管理員可以讀取的/etc/shadow檔案。
- /var/log/secure：檔案用於記錄與安全相關的所有事件，包含用戶登入紀錄。
- ./bash_history：使用者曾經下過的指令。
- ~/.ssh/known_hosts：連線至對方主機後，會記錄對方主機的指紋。這樣做是為了在未來的連線中能夠識別和驗證該主機。以防範中間人攻擊。
- /var/log/wtmp：使用者的登入歷史紀錄

常見攻擊:

- 緩衝區溢位(Buffer Overflow):攻擊者針對程式設計缺陷，在某個資料超過了處理程式限制的範圍時，破壞程式執行、趁著中斷之際取得程式或是系統的控制權，進而入侵系統，竊取資料，甚至造成主機當機的現象。
- SQL注入(SQL Injection):攻擊者利用網站應用程式的安全漏洞，將惡意的SQL代碼插入到後端資料庫執行的查詢中。這可能導致未經授權的資料存取或操作，例如繞過登入認證、提取、修改、刪除資料庫中的資料，甚至是執行管理員級別的任務。

常見攻擊-續：

- 重送攻擊(Replay Attack)：在這種攻擊中，攻擊者截獲網路通訊中的有效封包並重新傳送它們，以期欺騙系統進行未經授權的操作。例如，攻擊者可能會截獲一個用戶對銀行的交易認證封包，然後重送這些封包來進行不正當的金錢轉移。
- 阻斷式攻擊(Denial of Service Attack)：攻擊者發起大量的請求或封包，超過網站或網路服務的處理能力，導致合法用戶無法存取該服務。如果是分散式(distributed)阻斷式攻擊（DDoS），攻擊會來自多個源頭，使得防禦更加困難。這種攻擊的目的是使網站或服務不可用，影響其正常營運。

常見攻擊-續:

- 中間人攻擊(MitM):中間人攻擊發生時，攻擊者秘密地介入通訊雙方之間，攔截、修改或轉發雙方的通訊資料。這種攻擊方式可能讓攻擊者截獲敏感資訊，如登入憑證和信用卡信息，或者在通訊過程中注入惡意資訊。
- ARP欺騙(ARP Poisoning):ARP欺騙是透過發送偽造的ARP到區域網路內，目的在於將攻擊者的MAC地址與網內其他主機的IP地址關聯起來。這使得攻擊者能夠接收本該發送給這些主機的流量，常用於執行中間人攻擊。
- SYN Flooding網路阻斷服務攻擊:用戶傳用SYN封包給伺服器，收到SYN/ACK之後，不傳送ACK回伺服器，使三項交握永遠無法完成。

常見攻擊-續:

- DNS放大攻擊(DNS amplification attack):DNS放大攻擊通過利用公開可訪問的DNS伺服器，發送大量DNS查詢請求並偽造受害者的IP地址，迫使DNS伺服器向受害者發送大量回應。這不僅消耗受害者的網絡頻寬，也給DNS伺服器帶來負擔，屬於分散式拒絕服務（DDoS）攻擊的一種。
- 暴力破解(Brute Force Attack):暴力破解攻擊是通過不斷嘗試猜測密碼，來獲得未授權訪問的攻擊方式。攻擊者通常使用自動化工具，嘗試所有可能的密碼組合，直到找到正確的密碼。這種攻擊方式對於弱密碼尤其有效。
- TCP/IP 連線劫持(Session Hijacking):取得要劫持連線的 TCP 序號(Sequence Number)，與受害主機 可建立網路連線，偽裝成受害主機，發送特定 TCP 序號的封包。

常見攻擊-續:

- 零日攻擊(Zero Day Attack):零日攻擊是指利用軟體中未公開的安全漏洞進行的攻擊。因為這些漏洞在被發現並修復之前是未知的，所以稱為「零日」。攻擊者利用這些漏洞可以繞過安全防護措施，進行數據竊取、系統控制等惡意行為。
- 社交工程(Social engineering):社交工程是一種安全攻擊手段，主要是透過心理操控的技巧誘使人們放棄機密資訊或進行某些行為，而不是通過傳統的駭客技術來獲取存取權限。這種攻擊手法利用人類的自然傾向和情感弱點，例如好奇心、貪婪、恐懼或對權威的尊重，來誘騙受害者執行攻擊者的指示。
- 垃圾搜尋攻擊(Dumpster Diving):是指攻擊者搜尋企業或個人未妥善處理的廢棄物（如紙質文件、光碟、硬碟或其他存儲媒介），以尋找有價值的資訊的行為。這種資訊可能包括個人識別資訊（PII）、財務記錄、密碼列表、內部通訊、商業秘密或任何其他可用於進行進一步攻擊的敏感數據。

常見攻擊-續:

- 跨站指令碼(Cross Site Scripting, XSS)攻擊:XSS攻擊利用了網站對用戶輸入資料處理不當，從而在其他用戶的瀏覽器中執行惡意腳本。例如:在一個心情留言板上，攻擊者留下一則包含惡意 JavaScript 代碼的留言。當其他用戶瀏覽這些留言時，他們的瀏覽器會執行該代碼。
- 跨站請求偽造(Cross Site Request Forgery CSRF):CSRF攻擊通過誘導已登錄用戶在不自知的情況下執行攻擊者預定的操作。例如，攻擊者在一個惡意網頁上放置一個隱藏的轉帳表單，指向一家銀行的轉帳URL，並設置好收款人(攻擊者)和金額。當已登錄銀行的用戶訪問這個惡意網頁時，表單自動提交，由於用戶已驗證，銀行系統錯誤地處理這個轉帳請求。
- Rootkit:Rootkit是一種惡意軟體(或一組軟體)，設計用來為攻擊者提供對目標計算機系統或網絡中一台或多台機器的持久性隱蔽訪問。Rootkit主要目的是隱藏自身和其他惡意活動，避免被安全軟體檢測到，從而允許攻擊者長期控制或監視受感染的系統。

常見攻擊-續:

- 網路釣魚(Phishing):網路釣魚是一種社會工程手法，攻擊者通過發送看似來自合法來源的電子郵件、簡訊或社交媒體訊息，試圖誘騙收件人提供個人資訊，如用戶名、密碼、信用卡資料等。這些訊息通常包含一些緊急或誘人的信息，促使受害者點擊連結，導向假冒的網站，進而騙取受害者的個人或財務資訊。
- 捕鯨(Whaling):捕鯨是針對高階主管或重要個體的釣魚攻擊，所以又稱為「高價值目標釣魚」。這種攻擊通常涉及更加精心設計的郵件或訊息，目的是欺騙公司的高層管理人員，如CEO或財務主管，因為他們能夠存取敏感的公司資訊或進行重大的財務操作。

常見攻擊-續:

- 魚叉式釣魚(Spear Phishing):魚叉式釣魚是一種更加針對性的釣魚攻擊，攻擊者會事先收集目標個體的個人資訊，然後定製化的欺詐郵件或訊息，使其看起來更具有個人相關性和說服力。由於這種攻擊方式在準備上需要更多的功夫，因此通常用於針對具體個體或小型群體，以提高成功率。
- 聲音釣魚(Vishing):聲音釣魚是通過電話系統進行的釣魚攻擊，攻擊者可能會偽裝成銀行、技術支援或其他服務提供者的工作人員，試圖誘騙受害者提供個人資訊或直接進行金錢轉賬。這種攻擊利用了人們對電話通訊的信任，以及在電話中難以識別對方身份的特性。

常見攻擊-續：

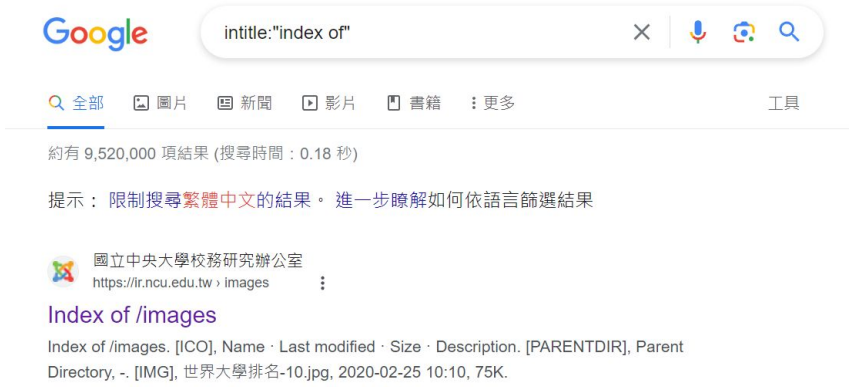
- 勒索軟體(Ransomware)：旨在加密受害者的檔案並要求贖金。勒索軟體通常透過電子郵件、網路釣魚攻擊或惡意軟體感染電腦。一旦電腦感染勒索軟體，受害者將無法存取其檔案。勒索軟體會顯示一條訊息，要求受害者支付贖金以解密檔案。由於加密軟體經常會變形，因此很難被防毒軟體(基於pattern)發現，著名的WannaCry勒索病毒使用伺服器訊息區塊（SMB）漏洞(CVE-2017-0143、CVE-2017-0148)攻擊微軟作業系統，微軟公司已於2017年3月14日在TechNet發佈「MS17-010」的資訊安全公告，並向使用者推播了Windows系統修復修補程式「KB4013389」封堵此漏洞。此漏洞是使用永恆之藍(EternalBlue)的技術。
- 勒索軟體的強大之處在於其使用非對稱金鑰加密技術來加密受害者的檔案，這種技術涉及一對金鑰：公開金鑰和私人金鑰。在感染過程中，公開金鑰被用來加密受害者的檔案，而私人金鑰，作為解密這些檔案的唯一鑰匙，則被攻擊者安全地保管。攻擊者會要求支付贖金，作為交換私人金鑰以解密檔案的條件。這種加密方法的關鍵在於，沒有私人金鑰，就算擁有公開金鑰也無法解密檔案，因此即使受害者使用最新的防毒軟體，也無法破解加密，只能考慮是否支付贖金以取回自己的資料。

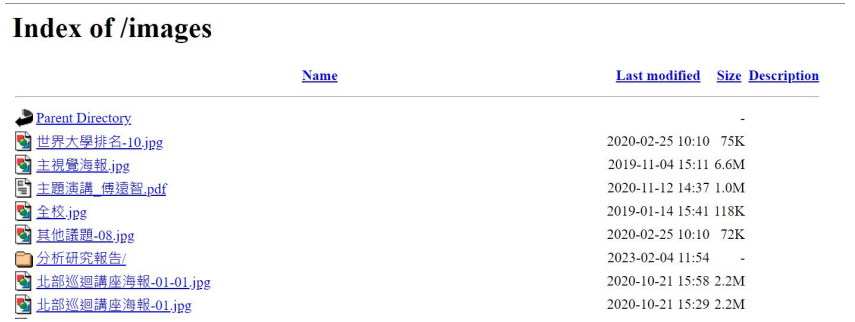
常見攻擊-續:

- Polymorphic Virus:是一種多形病毒，它會在每次感染時對自身的程式碼進行變異。Polymorphic Virus通常會使用變形引擎來生成新的程式碼。
- IP 位址欺騙(IP address spoofing):是一種網絡攻擊技術，攻擊者在此技術中偽造發送封包的來源IP地址，使其看起來像是來自受信任的來源IP地址。
- 搜尋引擎攻擊(Google Hacking):利用搜尋引擎（如Google）進行高級搜尋查詢，以發現網站的安全漏洞、敏感資訊泄露、公開的敏感目錄或文件等。這種技術是通過使用特定的搜尋語法（稱為Google Dorks）來實現的，這些語法可以幫助攻擊者快速找到網路上的漏洞資訊或敏感資訊。

常見攻擊-Google Hacking

- site: - 指定要在特定網站或域中搜索的資訊。例如，site:example.com 將只顯示來自 "example.com" 的結果。
- filetype: - 搜索特定文件類型。例如，filetype:pdf 將找出所有的 PDF 文件。
- intitle: - 搜索在網頁標題中出現的文字。例如，intitle:"index of" 可以用來尋找開放目錄。
- inurl: - 搜索 URL 中包含特定文字的頁面。例如，inurl:admin 將會找出 URL 中含有 "admin" 的頁面。
- intext: - 搜索網頁正文中出現的特定文字。例如，intext:confidential 可以用來查找包含 "confidential" 文字的頁面。





常見攻擊-續：

- 電腦病毒(Virus)：電腦病毒具有散播、隱藏、感染、潛伏及破壞等特性，附著於執行檔或文件，透過用戶互動（如開啟檔案）傳播。
- 木馬程式(Trojan Horse)：偽裝成合法軟體或隱藏在合法軟體之中，騙取使用者的信任以執行惡意活動。木馬程式的目的可能包括竊取資料、安裝更多惡意軟體或創建一個系統漏洞等，但它本身不會自我複製或擴散到其他文件。
- 蠕蟲(Worm)：會不斷複製，並利用網路感染其他主機，不需要用戶互動，利用網絡漏洞感染其他系統。
- 後門程式(Backdoor)：是一種允許遠端未經授權存取的惡意程式。它創建了一個隱秘的入口，使攻擊者可以繞過正常的身份驗證程序，遠端控制受感染的電腦。後門可以由其他惡意軟體（如木馬）安裝，或者由攻擊者直接利用系統漏洞創建。

常見攻擊-續:

- 字典攻擊法(Dictionary Attack):這種攻擊方法使用一個預先編制的詞彙列表(即“字典”),這個列表包含了大量可能的密碼,攻擊者將這些密碼一一嘗試,以尋找正確的密碼。這個列表可能包括常用的、猜測的或先前洩露的密碼。
- 彩虹表攻擊(Rainbow Table Attack):彩虹表是一種預先計算出的,用於加密演算法雜湊值與其對應明文密碼之間映射關係的巨大資料表。透過查找加密後的雜湊值,如果這些值存在於彩虹表中,攻擊者可以迅速找到對應的明文密碼,而不需要進行現場計算。
- 密碼潑灑(Password Spraying)攻擊:是一種猜測密碼的攻擊方式,不同於傳統的暴力破解攻擊(嘗試一個帳號的許多密碼),密碼潑灑針對多個用戶嘗試同一個或少數幾個常見的弱密碼。

常見攻擊-續:

- Smurf Attack：Smurf攻擊是通過向網路廣播地址發送大量的ICMP請求（Echo請求）封包，並將返回地址偽裝成目標機器的IP地址，從而使得回應的Echo回應封包洪水般地返回到目標機器上，導致目標機器或網路服務不可用。
- Land Attack：攻擊是一種拒絕服務（DoS）攻擊，攻擊者在TCP/IP封包的標頭中將目的地IP地址和來源IP地址設置為相同的值，並將該封包發送到目標系統。當目標系統接收到這樣的封包時，可能會導致系統崩潰或重啟，因為它試圖回應自己，從而進入一種無限循環。
- Fraggle Attack：Fraggle攻擊通過UDP協定發送大量的封包至網路的廣播地址，並將封包的來源地址偽造為攻擊目標的IP地址。

常見攻擊-續:

- UDP Flood Attack：UDP洪水攻擊是通過向目標系統或網絡發送大量的UDP封包來耗盡目標的資源，從而導致拒絕服務。這種攻擊不關心封包是否到達有效端口。
- ICMP Flood Attack：ICMP洪水攻擊（又稱為Ping洪水攻擊）是通過向目標發送大量的ICMP（網際網路控制消息協議）Echo請求（即Ping請求），試圖耗盡目標的處理能力和網路頻寬，從而使正常的請求無法被處理。
- Teardrop Attack：是利用 IP 分組的重組機制。IP 分組在傳輸過程中可能會被分割成多個片段，到達目的地後再進行重組。攻擊者會利用這一點，發送具有重疊或衝突的 IP 分組片段，導致主機在重組時發生錯誤，進而耗盡主機的資源。

常見攻擊-續:

- 鍵盤側錄:也稱為鍵盤記錄或鍵盤監聽，是一種監控技術，通常被用於惡意目的。這種技術涉及攻擊者透過惡意軟軟體(稱為鍵盤側錄器或鍵盤記錄器)來記錄或攔截在電腦鍵盤上輸入的所有按鍵資訊。這些記錄下來的資訊可能包括敏感資料，如用戶名、密碼、信用卡資訊、個人對話等，之後這些資料會被未經授權地傳回給攻擊者。
- 憑證填充攻擊(Credential Stuffing):是一種自動化的網絡攻擊手段，攻擊者利用先前從其他網站洩露的用戶名和密碼，試圖在多個網站上登入，因為很多用戶會在不同的網站上重複使用相同的登入憑證。
- 安全設定錯誤(Security Misconfiguration):這是一種常見的安全問題，發生於應用程式、資料庫、Web伺服器、平台等未被正確配置的情況下。顯示過多的錯誤訊息(如堆疊追蹤)給終端使用者，可能會無意中洩露關於應用程式的內部結構、底層技術、資料庫欄位等機敏資訊，從而給攻擊者提供可利用的資訊。

常見攻擊-續:

- Ping of Death : 攻擊者會發送一個或多個ICMP數據包給目標系統，這些數據包的大小超過了IP協議所允許的最大封包大小（65,535）。當這些過大的封包到達目標系統時，由於系統無法正確處理這種異常大小的封包，可能導致系統崩潰或重新啟動。
- 複製型釣魚（ Clone Phishing）: 攻擊者使用某些方法密切監視受害者收件匣。攻擊者會收受害者近期電子郵件最好有連結或附件並進行複製偽造。
- Typosquatting Attack（誤植域名攻擊）: 這是一種被動攻擊形式，攻擊者註冊與知名域名相似的域名，當用戶不小心輸入錯誤的網址時，可能不經意地訪問到這些惡意網站。雖然這種攻擊可以用於進行釣魚等主動攻擊，但其本身更多地關注於利用用戶的錯誤輸入來誘導他們訪問偽造的網站，而不是直接對目標系統進行攻擊。

常見攻擊-續:

- 密碼撞庫攻擊（Password Spraying）: 攻擊者在這種攻擊中會選擇一個或少數幾個常見的弱密碼，然後嘗試將這些密碼用於大量用戶帳戶，以尋找能夠成功登錄的帳戶。
- 進階持續性威脅(Advanced Persistent Threats, APT): 駭客為了追求最大利益，將亂槍打鳥的隨機攻擊轉換成目標式攻擊，具有隱匿性高且長期潛伏於目標系統的特性，潛伏期可以只是幾天，也可能長達一年半載，遭受攻擊後，被害者多數只能盡快修補漏洞並設定災害停損點，無法有效根除攻擊。

軟體測試分類

- 單元測試：主要測試單一單元是否運作正常。目的是確保單個單元符合預期的設計。應由開發人員進行，因為他們最熟悉程式碼的設計和實現。
- 整合測試：是對軟體的各個單元進行組合測試，以確保它們能夠正常地相互協作。
- 系統測試：主要測試整個軟體系統是否符合功能需求。目的是確保軟體能夠滿足用戶的需求。複雜度較單元測試高。可以由開發人員或軟體品保工程師進行，但軟體品保工程師通常具備更全面的測試經驗和知識。

軟體測試-續

- 驗收測試：驗收測試是軟體開發過程的最後一個階段，它是由用戶或用戶代表進行的測試，以驗證軟體是否滿足實際應用需求和規格說明書的要求，例如功能測試就是規格說明書上的每一項功能需求測試。驗收測試的目標是確保軟體能夠在實際環境中正常運行。
- 白箱測試：一種測試方法，它在測試時會考慮軟體的內部結構或運作。白盒測試的目標是確保軟體的內部結構結構的正確性和符合設計要求，更容易發現邏輯性缺失。例如：Code Review和原始碼掃描。
- 黑箱測試：一種測試方法，它在測試時不考慮軟體的內部結構或運作。黑盒測試的目標是驗證軟體是否符合需求規格說明書中的規定，例如：滲透測試。

惡意程式分析

- 靜態分析：態分析是一種不執行程式碼的分析方法，它通過檢查程式碼、配置和資料結構來識別軟體中的錯誤、漏洞或不符合特定編碼標準的代碼。這種分析可以在軟體開發的早期階段進行，有助於快速發現問題，減少後期修正的成本。
- 動態分析：動態分析與靜態分析相反，它涉及在實際執行時分析和評估程式的行為。透過監視程式的運行時行為，動態分析可以幫助識別如記憶體洩漏、執行時錯誤、非預期行為和效能問題等問題。

惡意程式分析

- 沙盒分析：沙盒分析是一種特殊類型的動態分析，通常用於測試可疑的或惡意的軟體程序，以觀察其行為而不影響主機系統。在沙盒環境中，程式被隔離執行，從而能夠安全地分析其行為，包括網路活動、文件操作、註冊表更改等，而不會對實際的操作系統或網絡環境造成危害。沙盒分析尤其對於識別和評估惡意軟體、病毒、木馬和其他網絡威脅非常有效。

常見工具

- Tenable(Nessus)、OpenVAS、OSV-Scanner、Rapid7(InsightVM)：主機弱點掃描工具。
- Burp Suite、Appscan、OWASP(ZAP)、Rapid7(InsightAppSec)：Web應用程式弱點掃描。
- Nmap：可用於發現網路上的主機和服務。
- Wireshark：抓取封包的工具。
- Aircrack-ng：無線網路安全的工具。
- Kali Linux：已經安裝好很多工具的Debian的Linux發行版。
- Metasploit：開發和執行針對遠程目標主機的漏洞利用代碼，滲透測試工具。
- SQLmap：一個自動化的SQL注入和資瞭庫接管工具。
- John the Ripper：一個快速的密碼破解工具。

常見工具-續

- NC(NetCat)：建立後門程式工具。
- Mimikatz：用於攻擊或竊取 Windows 憑據的工具。
- 中國菜刀(China Chopper)：是一款廣為人知的Webshell管理工具，主要被網絡攻擊者用於遠程控制和管理已經被攻破的Web服務器。
- Masscan：端點掃描工具。
- Tcpreplay：可以傳送封包的工具。
- Hping：類似ping功能但是功能更強大。
- ngrep：封包分析工具。
- OSSIM：SIEM軟體。

儲存設備差別

- 直接附加存儲 (DAS - Direct Attached Storage)：這是將儲存設備直接連接至電腦或伺服器的方法，如內部或外部硬碟。不支援遠端存取或多台電腦共享。
- 儲存區域網路SAN(Storage Area Network)：SAN 通過光纖通道 (Fibre Channel, FC) 或 IP 網路（例如使用 iSCSI）提供伺服器與儲存設備間的高速連結。它支援Block Level的存取，使伺服器可以將SAN上的存儲設備視為本地硬碟使用。SAN 適合於需要高性能和高可靠性的企業級應用，但成本相對較高。
- 網路附接儲存NAS(Network Attached Storage)：NAS 通過標準的 IP 網路連接，提供File Level的存取。它允許多台電腦共享相同的存儲空間，適合檔案共享和資料備份。NAS 裝置簡單易用，成本低於 SAN，支援多種檔案共享協議如SMB/CIFS（適用於Windows環境）和 NFS（適用於UNIX/Linux環境）。

常見攻擊方式考題

- SQL Injection攻擊：
  - 關鍵字：‘ OR ’1‘=’1‘, ’; %27+OR+%271%27%3D%271%27+ (URL編碼型式)
  - 當看到題目中涉及到直接將用戶輸入拼接到 SQL 查詢語句中時，應該考慮 SQL 注入攻擊的可能性。
- Cross-site Scripting (XSS - 跨站腳本攻擊)：
  - 關鍵字：<script>alert(’abc’);</script>, <OMG SRC=javascript:alert(’lol’)>
  - 題目中如果提到在網頁上插入未經驗證或淨化的用戶輸入，可能指向 XSS 攻擊，常為使用JavaScript。
- Directory Traversal (目錄遊走)：
  - 關鍵字：../../, ../etc/passwd, ..%2F..%2F. (URL編碼型式)
  - 當題目描述涉及到通過修改URL或文件路徑來訪問不應該被訪問的文件或目錄時，即指目錄遊走攻擊。
- Cmd Injection(命令注入)：
  - 關鍵字：&, ;, |, &&, ||, $(command), `command` (Linux常用sh，Window常用cmd)
  - 當應用程序將用戶輸入直接用於系統命令的構造時，而沒有適當的檢查或淨化，就可能發生命令注入。攻擊者可以利用這種漏洞執行任意命令，從而潛在地接管系統或獲取敏感資訊。

URL編碼

!	%21	)	%29
#	%23	*	%2A
$	%24	+	%2B
&	%26	,	%2C
'	%27	/	%2F
(	%28	:	%3A

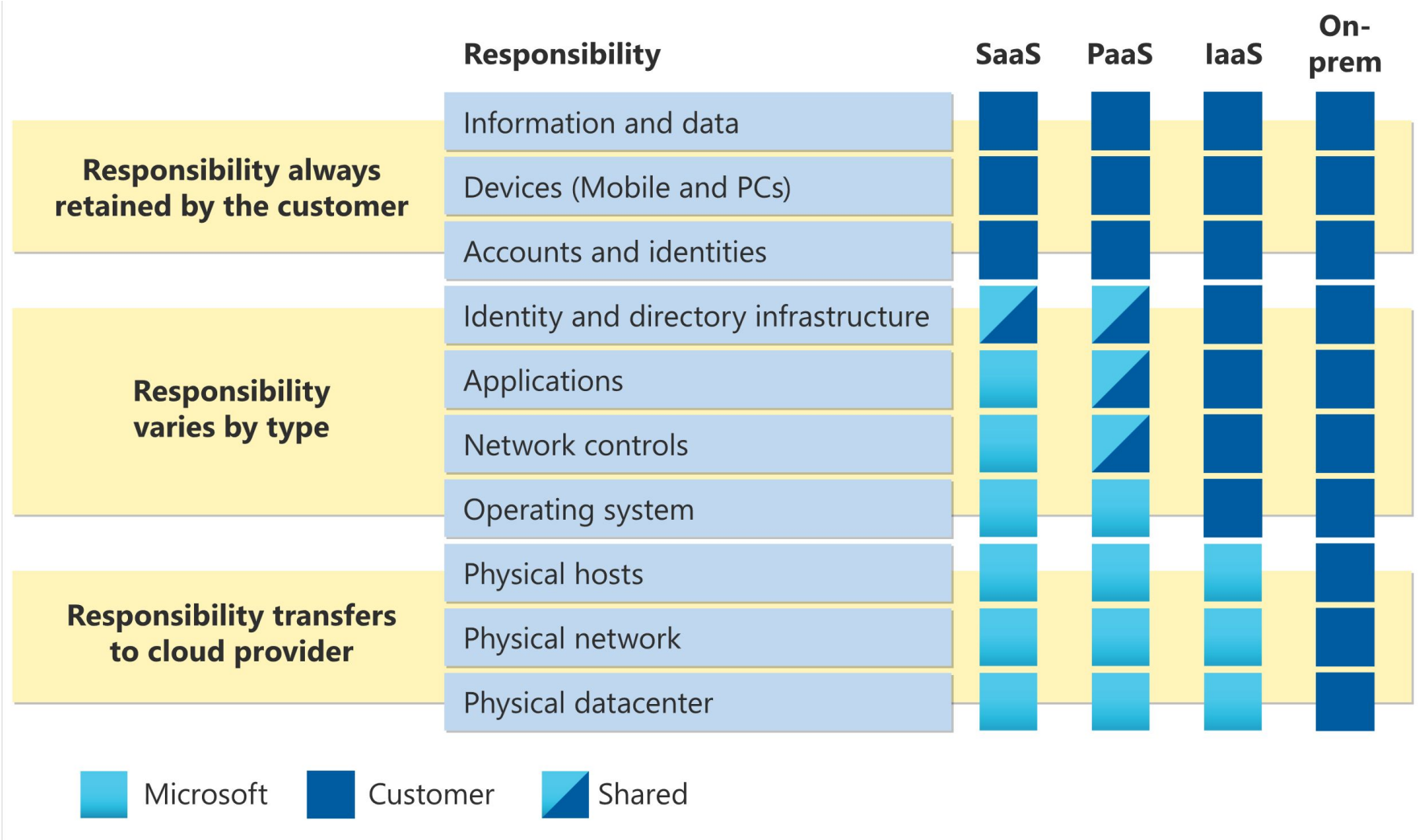
雲端運算

- 由美國國家標準技術研究院（National Institute of Standards and Technology, NIST）所定義的雲端運算的五項關鍵特徵。
  - 隨需自助服務（On-demand self-service）：用戶可以自行自動獲取計算資源，如伺服器時間和網絡存儲，而無需人工互動。
  - 廣泛的網路存取方式（Broad network access）：能夠透過網絡使用標準機制在各種裝置上存取服務，例如：電腦、手機、平板等。
  - 資源池共享（Resource pooling）：供應商利用一個多租戶模型，將計算資源池化以服務多個消費者，物理和虛擬資源動態分配和重新分配根據消費者需求。
  - 快速且彈性的架構（Rapid elasticity）：資源可以彈性地被分配和回收，有時甚至是自動的，以便快速擴展和縮減以匹配需求，對外呈現無限資源的感覺。
  - 可量測的服務（Measured service）：雲系統自動控制和優化資源的使用，利用一個計量能力。這種資源使用可以被監控、控制、報告，提供透明度給雙方。

雲端運算-續

- 軟體即服務(Software as a Service , SaaS)：電子郵件(Gmail)或Dropbox服務。
- 平台即服務(Platform as a Service , PaaS)：提供開發、測試、交付和管理應用程式的平台。
- 基礎架構即服務(Infrastructure as a Service ,IaaS)：建立雲端虛擬機。
- 私有雲：企業自己建的機房，僅供企業使用。
- 公有雲：AWS、Azure、GCP三大公有雲。
- 混合雲：同時使用上述兩種型態。
- 社區雲：基於某些目的一起建立使用，比方說教育部建立教育雲。

雲端運算共享責任


Responsibility
SaaS
PaaS
IaaS
On-prem
Responsibility always retained by the customer
Information and data
Devices (Mobile and PCs)
Accounts and identities
Responsibility varies by type
Identity and directory infrastructure
Applications
Network controls
Operating system
Responsibility transfers to cloud provider
Physical hosts
Physical network
Physical datacenter
Microsoft
Customer
Shared

常見資安名詞:

- MDM(Mobile Device Management):為確保手機安全性及方便管理，許多公司使用 MDM 的軟體或平台，用來限制手機功能或提供遠端資料抹除能力。
- EDR (Endpoint Detection and Response):EDR 解決方案專注於監控終端裝置（如個人電腦、手機等）上的活動，以偵測、調查和回應惡意軟體和攻擊。EDR 系統能夠提供即時分析和警報，幫助識別和阻止安全威脅。
- SIEM (Security Information and Event Management)SIEM 技術結合了安全資訊管理（SIM）和安全事件管理（SEM），提供即時監視、事件記錄、資料聚合、事件關聯分析等功能。SIEM 解決方案用於集中管理企業的安全警報，透過分析來自不同來源的日誌和事件資料，以識別潛在的安全事件。

常見資安名詞-續:

- DLP (Data Loss Prevention)DLP 技術和策略旨在防止敏感或重要資料的未授權訪問和傳播。DLP 解決方案可以監控和控制數據端點、網絡傳輸和儲存位置的資料流動，幫助確保敏感資料不會因外泄或被竊而導致合規性問題或商業損失。
- WAF (Web Application Firewall)網頁應用程式防火牆:專為保護網頁應用程式免受跨站腳本、SQL注入等攻擊的安全技術。
- IPS/IDS (Intrusion Prevention Systems/Intrusion Detection Systems)入侵防禦系統/入侵偵測系統:這些系統用於監測網絡或系統活動以識別惡意活動、記錄資訊、報告並自動預防或回應安全威脅，兩者最大的差別是，IDS僅監控不阻擋，IPS為監控也阻擋。
- 生成樹協定(Spanning Tree Protocol, STP):由於廣播封包在L2交換器上有所有port都傳送的特性，如果交成loop會造成無線迴圈，因此STP會產生一棵虛擬樹，對於可能會產生迴圈port進行阻擋。

常見資安名詞-續:

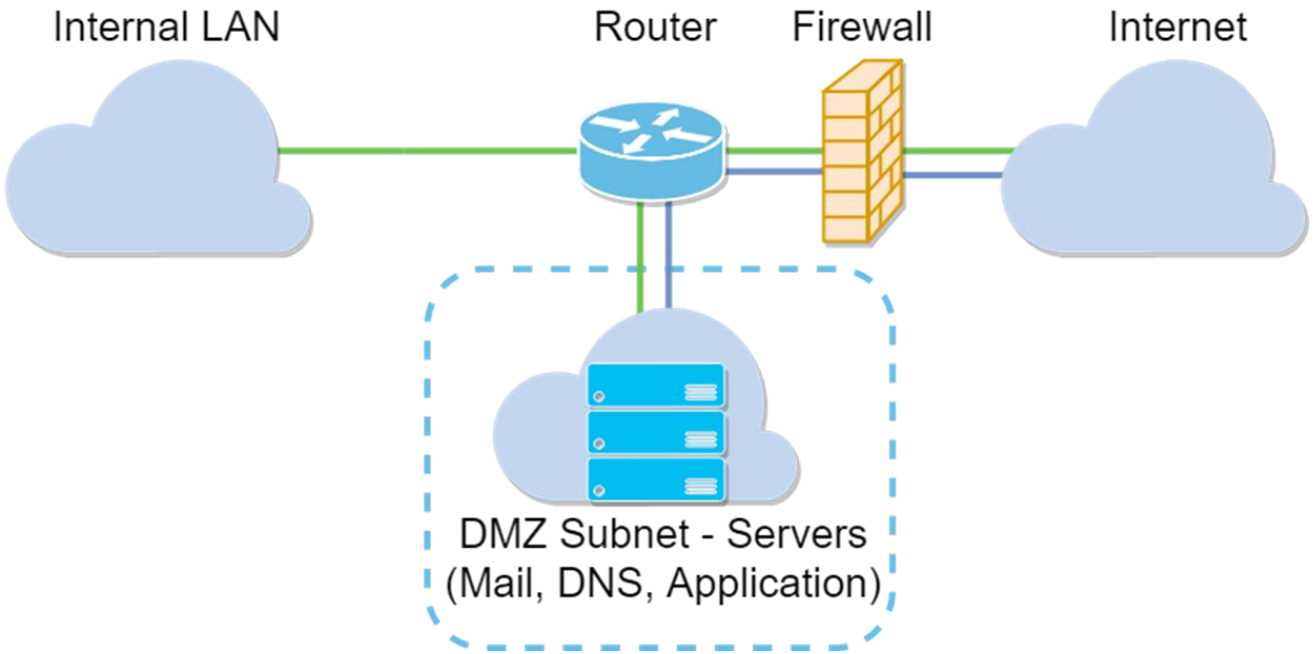
特性	防火牆	WAF（網頁應用程式防火牆）
操作層級	網絡層/傳輸層（第3層和第4層）	應用層（第7層）
保護目標	保護網絡不被未授權訪問	保護Web應用免受應用層攻擊
防範威脅	端口掃描、DoS攻擊等	SQL注入、XSS、目錄遊走、CSRF等
部署位置	網絡邊緣	Web服務器前面

常見資安名詞-續:

- SOC (Security Operations Center):安全運營中心:專門的團隊負責實時監控、評估和防禦組織內外的資訊安全威脅。
- 網絡閘道安全(Web Security Gateway):控制進出企業網絡的網絡流量，以保護組織免受惡意軟體、網站和其他網絡基礎威脅的侵害，例如公司上網都要透過代理伺服器，過濾黃賭毒網站。
- VPN (Virtual Private Network):虛擬私人網絡:VPN技術允許安全地通過公共網絡傳輸數據，為遠端使用者提供安全的連線方式，好像中間傳輸有一條加密通道，例如家裡連到公司辦公。
- UTM（Unified Threat Management，統一威脅管理）是一種綜合性的網絡安全解決方案，類似防火牆但是多了很多功能，例如:IPS、VPN和病毒過濾。

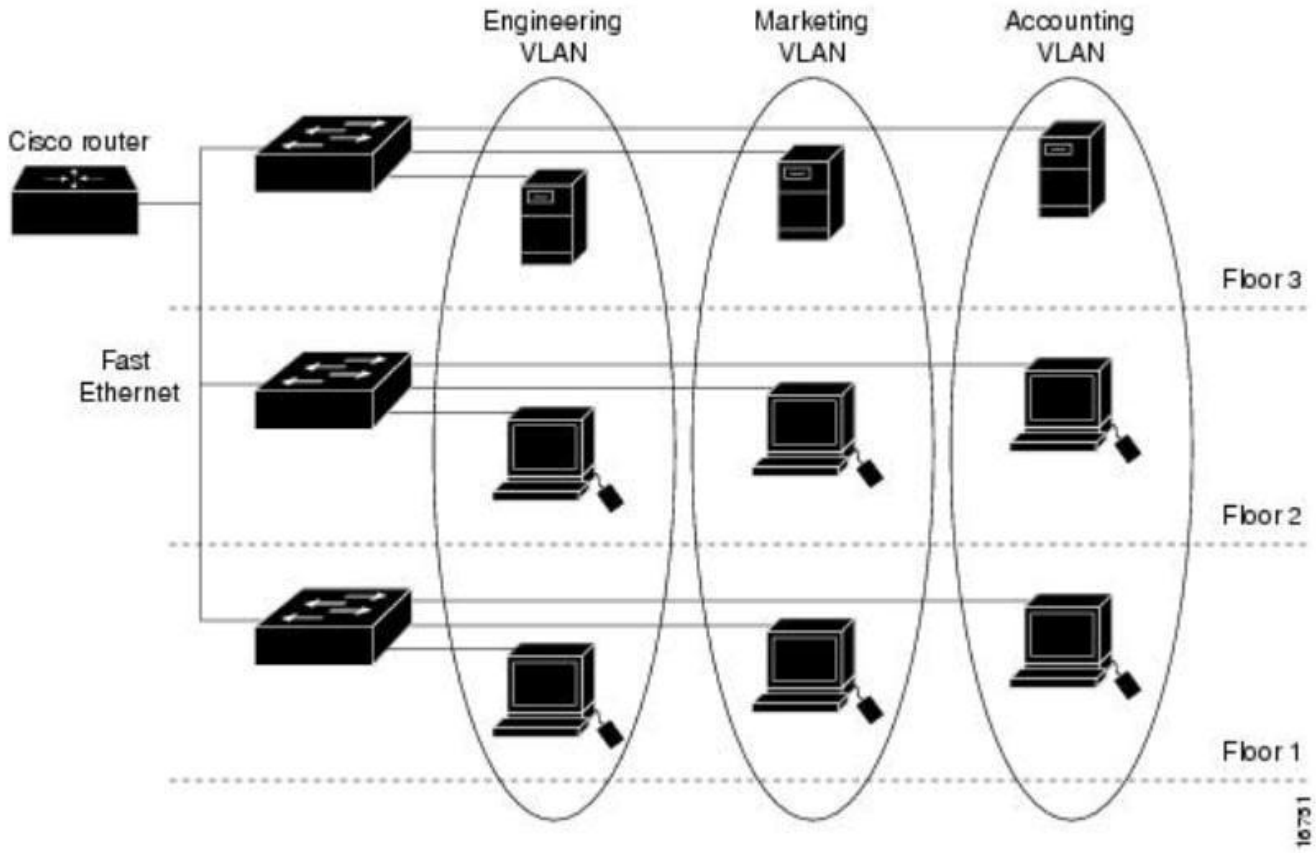
常見資安名詞-續:

- 非軍事區(Demilitarized Zone, DMZ):防火牆限制外部網際網路使用者，只可存取放置組織公開資訊(對外網站)的區域，不可進入內部網路，其放置組織公開資訊的區域。



常見資安名詞-續:

- VLAN（Virtual Local Area Network，虛擬局域網）是一種網絡技術，它允許將一個物理網路分割成多個虛擬網絡，使得在同一個物理網絡基礎設施上的設備可以被分組到不同的虛擬網絡中。這樣，即使設備在物理位置上相互接近，它們也可以像在不同網絡中一樣進行隔離，從而提高了網絡的安全性和管理的靈活性，VLAN之前只能進行跨網段(L3)的傳遞，每個VLAN都是一個獨立的廣播域(Broadcast Domain)。



常見資安名詞-續:

- 蜜罐(Honeypot):偽裝成有價值的網路或電腦系統，並設置漏洞，誘使駭客攻擊，可用來取得電腦病毒樣本，或是確定是否有被攻擊，非任何連線連線蜜罐的行為都是可疑的，因為有可能會誤連，通常設置在非正式的產品運作環境之中。
- 網路地址轉換(Network Address Translation, NAT):NAT是一種網路服務，用於解決公有IP地址不足的問題。它允許多個設備共享一個公有IP地址進行上網，透過將私有（內部）IP地址轉換為公有（外部）IP地址，從而實現與外部網路的通信。同時，當外部請求需要訪問公司內部資源時（如訪問公司網站），NAT也可以將公有IP地址轉換為私有IP地址，實現從外部到內部的連接。

常見資安名詞-續:

- 防毒軟體(Antivirus):無法偵測所有攻擊，常使用特徵（Signature）比對來偵測惡意程式，可監視作業系統的可疑活動與應用程式的行為，即使非Windows，如Mac電腦或Linux作業系統也建議安裝，防毒軟體使用「啟發/探索方法（Heuristic Method）」為不根據過往的特徵而是根據行為來判斷，可以偵測全新病毒。
- 資訊安全監控維運中心(Security Operation Center, SOC):是一個專門的部門，負責企業或組織的資訊安全監控、分析和防禦。SOC集中了專業的安全分析師和先進的技術，旨在實時監控和分析組織的安全狀態，以識別、評估和回應各種安全威脅。

駭客分類

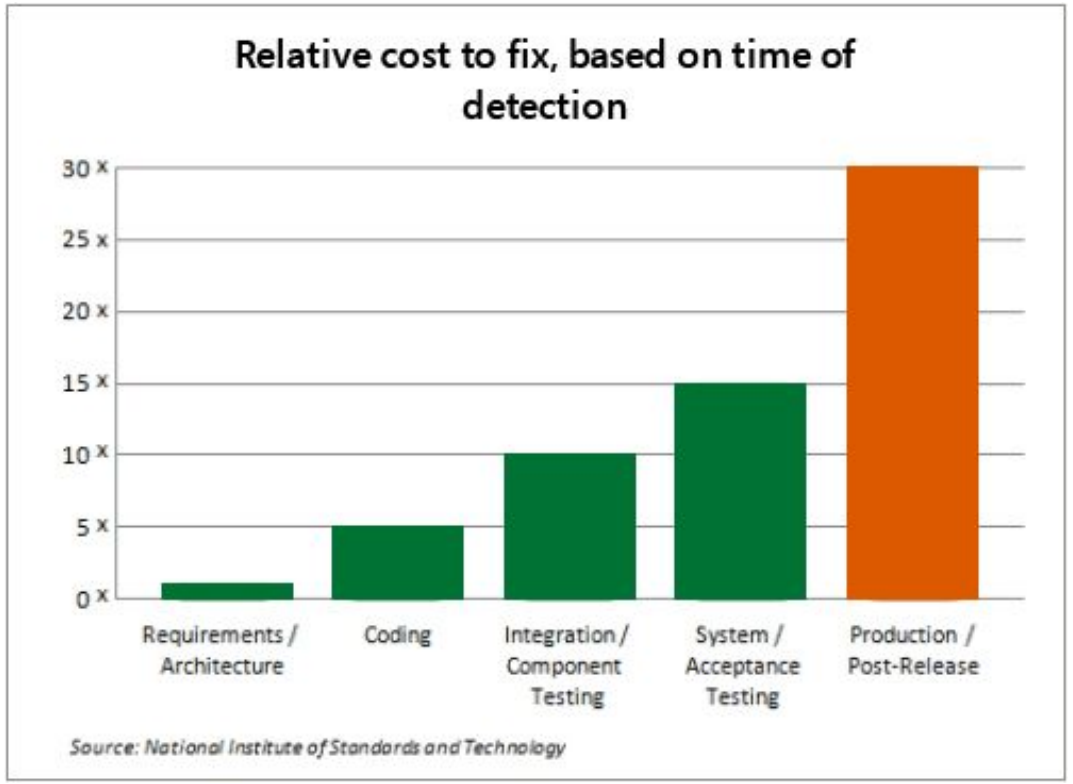
- 黑帽駭客(Black Hats)：黑帽駭客擁有卓越的電腦技能，常在深網（Deep Web）的陰影中活動。他們不僅能夠開發破壞性的工具和技術，而且經常涉足非法活動，如滲透未授權的系統，盜取資料或散布惡意軟體，動機多為個人利益或破壞。
- 白帽駭客(White Hats)：白帽駭客，亦稱為道德駭客，是資安領域的守護者。他們在組織的正式授權下執行滲透測試和安全評估，旨在識別和修補安全漏洞。發現漏洞時，他們會將這些發現回報給相關公司，幫助加強其網路和產品的安全防護，例如台灣的DEVCORE公司就是著名的白帽駭客公司，也在國際各大駭客競賽中得獎。

駭客分類

- 灰帽駭客(Gary Hats)：灰帽駭客的行為介於白帽和黑帽之間，他們的行動充滿矛盾。雖然他們可能在日間像白帽駭客一樣從事合法的安全測試，但在某些情況下，他們也可能未經授權地侵入系統，揭露安全弱點。不同於黑帽的破壞性意圖，灰帽的動機可能更多是出於好奇心或尋求公正，而非直接的財務利益。
- 腳本小子(Script Kids)：腳本小子是指那些依賴他人開發的攻擊工具進行惡作劇或發動攻擊的入門級駭客。他們缺乏深入了解所使用技術的原理，對於如何開發這些工具或攻擊的內部運作機制知之甚少。腳本小子通常是出於尋求刺激或想在同儕中炫耀而從事駭客活動。

SDLC測試左移

•根據國家標準技術研究院的資料，軟體缺陷的修復成本會隨著在開發生命週期中被發現的時間點而變化。越早發現並解決這些缺陷，其相對成本就越低。因此，強化安全的「測試左移」策略強調在軟體開發的每個階段—從需求設定和架構設計開始，到編碼、整合/組件測試、系統/接受測試，直至產品發布後—都要積極導入安全測試和檢查。這種策略不僅有助於減少潛在的安全風險，同時也能顯著降低後期修復的負擔和成本。



CVE

- CVE(Common Vulnerabilities and Exposures)：CVE全稱是「公共漏洞和暴露」，是一個廣泛使用的資訊安全漏洞的識別號系統。CVE系統提供了一個標準化的名稱，用來唯一地標識和參照特的安全漏洞。
- 目的：CVE的目的是讓資訊安全專業人員和工具能夠在討論、管理和解決漏洞時共享資訊。
- 結構：每個CVE識別號都是以"CVE-"開頭，後面跟著年份和一個唯一的數字，例如 "CVE-2021-34527"。
- 管理機構：CVE由MITRE公司管理，它是一個非盈利組織，與美國政府合作維護CVE系統。
- CVE對於溝通和數據交換是非常重要的，因為它提供了一個共通的語言來描述漏洞，無論是在不同的安全數據庫之間還是在不同的產品之間。

CVSS

- CVSS(Common Vulnerability Scoring System)：CVSS全稱是「公共漏洞評分系統」，是一種開放標準，用於評估和分數資訊安全漏洞的嚴重程度。
- 評分：CVSS給漏洞分配一個0到10的分數，這個分數反映了漏洞的嚴重性，10表示最嚴重。
- 計算：分數是根據一系列的標準指標計算得出，這些指標涵蓋了漏洞的利用難度、影響範圍、漏洞的複雜性等因素。
- 版本：CVSS存在多個版本，目前最常用的是CVSSv3，它提供了更精細的評分機制和更多的參數。
- CVSS分數幫助組織優先處理安全漏洞的修復工作，通過對不同漏洞的分數進行比較，可以決定哪些漏洞需要立即關注，哪些可以稍後處理。這個系統被廣泛用於各種安全產品和服務中，作為風險評估和緊急程度評定的標準方法。

CWE

- CWE（Common Weakness Enumeration）指的是「公共弱點枚舉」，它是一種用於描述計算機安全漏洞的標準化方法。CWE 提供了一個統一的、標準化的弱點類型集合，幫助軟體開發人員、安全研究人員以及資訊安全專業人員理解、討論和解決軟體中的弱點。
- 弱點分類：CWE 將弱點按類型分類，例如：輸入驗證錯誤、邊界條件錯誤、認證問題等。
- 弱點描述：對每個弱點類型提供詳細描述，包括其概念、可能的後果、示例以及如何避免。
- 實用工具：CWE 能夠幫助組織識別、編制和解決常見的軟體安全弱點，從而提高軟體的安全性。
- 改進安全性：它被設計用來指導安全工具的開發、促進安全研究和教育，以及作為安全審計和風險評估的基準。

OWSAP和NIST

- OWASP (Open Web Application Security Project)
- 一個著名的非營利組織，旨在提高軟體安全性，其發布的OWASP Top 10是描述網頁應用最危險安全風險的流行列表。
- NIST (National Institute of Standards and Technology)
- 美國國家標準與技術研究院，其發布的安全標準和指南，例如NIST Cybersecurity Framework，廣泛用於指導企業的資訊安全實踐。

原始碼掃描

- 原始碼掃描（Source Code Scanning）或原始碼是一種關鍵的安全實踐，它使軟體開發過程中能夠及早識別程式碼中的潛在安全漏洞。透過工具如FortifySCA、Checkmarx和SonarQube等，開發者能夠執行自動化的安全檢查，從而揭露出可能被惡意利用的弱點。
- 這些掃描工具通常提供可定制的報告，它們按照嚴重性將弱點分類為高、中、低等級，並常常參照如OWASP Top 10這樣的行業標準。原始碼掃描不僅限於開發的某個特定階段，它可以在從早期的需求分析到單元測試及之後的任何時候進行，支持多種程式語言，增加了掃描的通用性和便利性。
- 儘管原始碼掃描工具在識別諸如緩衝區溢出、SQL注入和跨站腳本攻擊等常見安全漏洞方面非常有效，但它們在處理複雜的業務邏輯瑕疵時可能不如手工審查(Code Review)有效。例如，自動化工具可能難以識別出飲料自動售賣機在某些情況下會同時掉落兩罐飲料的邏輯錯誤。這類問題可能需要更深層次的理解和分析，因此，在安全審計中結合手動審查是很重要的。

無線網路的加密協定

- WEP：WEP有著許多已知的安全漏洞，很容易被破解。使用RC4加密算法。由於其弱點，不再推薦使用WEP來保護無線網絡
- WPA：後來的標準仍然存在漏洞。引入了Temporal Key Integrity Protocol (TKIP) 加密方法，以及預共享金鑰（PSK）和企業級的身份驗證選項。
- WPA2：安全性高。WPA2引入了Advanced Encryption Standard (AES) 加密，提供了更強的安全性。成為了無線網絡安全的行業標準，包含個人和企業兩種模式，分別使用預共享金鑰（PSK）和802.1X基於EAP的身份驗證和RADIUS伺服器驗證。
- WPA3：安全性更高。WPA3提供了改進的資料加密和更強的防範密碼猜測攻擊的能力。引入了Simultaneous Authentication of Equals (SAE) 機制，用於提升初始鍵協商的安全性。WPA3同時提高了公開網絡的加密能力，透過個人化加密來保護用戶資料。

SSL和TLS差別

- SSL(Secure Sockets Layer)：SSL因Google發布在SSL 3.0中發現設計缺陷，故已不在使用。
- TLS(Transport Layer Security)：TLS跟SSL類似，都是因為HTTP本身不支援加密協定，因此必須透過TLS實現加密，目前TLS1.0和1.1陰不安全的關係僅建議使用TLS1.2以上。
- 即使是目前正在使用的協定，因為駭客破解的關係，也常常會宣告某些SSL Cipher Suite已經不安全，建議停用。
  - RC4：一度廣泛使用於TLS/SSL加密中，但由於其安全性問題，已被廣泛建議停用。
  - MD5：MD5 已被列為不安全的雜湊算法，建議停用。
  - SHA-1：SHA-1 已被列為不安全的雜湊算法，建議停用。

防範SQL Injection方法

- 對查詢字串進行字串過濾：僅對字串進行過濾，使用黑名單很難窮舉，有幫助但不建議使用。
- 參數化查詢：使用參數化查詢可以將使用者輸入的資料與SQL查詢分開。這樣，即使使用者輸入了惡意SQL查詢，也無法影響到資料庫
- Prepare Statement、Stored Procedures：使用SQL內建的參數化查詢可以將使用者輸入的資料與SQL查詢分開。這樣，即使使用者輸入了惡意SQL查詢，也無法影響到資料庫。
- 參數化查詢和Stored Procedures最大的差別是一個在程式端過濾，一個在SQL端過濾。

防範CSRF方法

- 使用圖形驗證碼(CAPTCHA)：
- 圖形驗證碼可以幫助區分人類和機器。在進行敏感操作之前，可以要求受害者輸入圖形驗證碼。如果受害者無法正確輸入圖形驗證碼，則可以阻止CSRF攻擊。

防火牆規則

- 順序由上到下，先進先出。
- 最後一條會預設Deny Any，因此是白名單。

狀態檢視防火牆

- 狀態檢視防火牆(Stateful Inspection Firewall)：此類型的防火牆會追蹤每個網路連接的狀態，包括封包的來源與目的地端口。例如，當一個從內部網路（使用端口60000）發起的連接嘗試訪問外部網站（通過443端口），狀態檢視防火牆會記錄此連接資訊，並允許從外部網站回到內部網路的封包通過。當連接結束時，防火牆會自動關閉這些特定端口的開放狀態，從而動態管理網路流量。
- 無狀態檢視防火牆(Stateless Inspection Firewall)：這種防火牆不追蹤網路連接的狀態。它僅根據預先設定的規則來允許或拒絕數據包的通過。這意味著，進出的封包都需要通過管理員事先設定的規則，否則可能導致連接失敗。無狀態檢視防火牆提供了基本的過濾功能，但缺乏更動態的連接追蹤能力。

交換器處理MAC動作

- MAC地址學習：當交換器接收到一個訊框（Frame）時，它會檢查來源MAC地址並將其與入口端口對應起來，記錄在內部的MAC地址表（MAC Table）中。這使得交換器能夠記住每個MAC地址是從哪個端口進來的。
- 動態學習：交換器的MAC地址表是動態生成的。隨著網絡上設備的加入、移動或移除，交換器會自動更新其MAC地址表。這一過程稱為動態學習，它確保了交換器能夠適應網絡結構的變化。
- 溢送（Flood）：當交換器接收到一個目的地MAC地址不在其MAC地址表中的訊框時，它會對這個訊框進行溢送，即將這個訊框發送到除了來源端口之外的所有端口。這確保了即使交換器還不知道特定MAC地址的正確端口，數據也能夠到達目的地。一旦回應訊框被接收，並且目的地MAC地址被學習，交換器便能夠將未來的訊框直接發送到正確的端口。

HTTP中GET、POST方法安全比較

- GET方法將資料附加在URL之後，作為查詢字符串的一部分，這使得資料在瀏覽器歷史、Web伺服器日誌、以及可能的中間網路節點中都是可見的。這種可見性增加了資料洩露的風險。
- https://news.google.com/search?q=iPAS&hl=zh-TW&gl=TW&ceid=TW%3Azh-Hant 例如範例中的iPAS就是因為查詢iPAS的新聞。
- POST方法將資料包含在請求的主體（body）中，這樣資料就不會顯示在URL中，相對於GET方法，這提供了更好的隱私。
- 例如：用戶註冊表單會使用POST方法，將資料包含在請求的主體（body）中。

Steganography 介紹

- Steganography（隱寫術）：是用於在普通消息中隱藏秘密消息的技術，通過隱蔽性提供安全性。隱寫術允許將秘密訊息或資料隱藏在圖片、影片、聲音檔案或任何其他“載體”文件中，使得第三方難以察覺到秘密訊息的存在。

(左边是原图二值化，右边是打上隐写的图二值化，显然右边隐写了信息)

防範XSS的方法

- 以白名單過濾輸入參數:這是一種更積極和更安全的方法，只允許預先定義的安全輸入通過。通過定義一個明確的列表，指定哪些類型的輸入是可接受的，這樣可以有效地防止未經授權或惡意的輸入造成的安全問題，包括XSS攻擊。

- 數位簽章是一種利用非對稱式加密技術來保證數位資訊真實性、完整性及不可否認性的技術。它允許一個人(或機構)使用自己的私鑰對資訊進行加密，而任何人都可以使用相對應的公鑰來驗證該簽章。在這個過程中，雜湊函數發揮了關鍵作用。首先，原始訊息通過雜湊函數生成一個固定長度的摘要(雜湊值)。這個雜湊值隨後被發送者的私鑰加密，形成數位簽章。這樣，數位簽章不僅包含了對訊息的加密認證，還包含了對訊息摘要的加密，從而保證了訊息的完整性和真實性。
  - 真實性：數位簽章確保訊息確實來自聲稱的發送者。通過對訊息摘要使用發送者的私鑰來創建簽章，並且只有與之匹配的公鑰才能解密驗證該摘要，接收者可以確信該訊息確實由持有相應私鑰的發送者所發。這意味著如果公鑰成功地解密了雜湊值並且與訊息的雜湊值匹配，則只有擁有對應私鑰的人才可能創建了那個簽章。
  - 完整性：數位簽章保證了訊息從發送到接收的過程中未被篡改。由於簽章是基於訊息的雜湊值生成的，任何對訊息的修改都會導致新的雜湊值與原始簽章中的雜湊值不匹配，從而使得驗證過程失敗。當接收者使用發送者的公鑰驗證簽章並計算訊息的雜湊值時，如果訊息在傳輸過程中被修改過，那麼驗證將不會成功。
  - 不可否認性：此外，數位簽章還提供了不可否認性，即發送者不能否認其已發送過的簽章過的訊息。由於簽章是用發送者的私鑰對訊息的雜湊值生成的，且該私鑰僅發送者擁有，因此可證明發送者曾發出該訊息。

HMAC

- HMAC 是一種用於資訊安全的技術，它結合了對稱式加密和雜湊函數的特點。
- 它的工作原理是通過一個共享的秘密鑰匙和一個雜湊函數對訊息進行加工，生成一個訊息認證碼（MAC）。這個MAC隨同原始訊息一起發送給接收方。接收方收到訊息後，使用相同的秘密鑰匙和雜湊函數對收到的訊息進行處理，生成一個新的MAC。然後，接收方將這個新生成的MAC與原始訊息中的MAC進行比較。如果兩者相同，則證明訊息是真實的（未被篡改），並且確認是由擁有共享秘密鑰匙的發送方發出的。
- 因此，HMAC 主要用於實現兩個目的：
  - 真實性：確認訊息是由擁有共享秘密鑰匙的發送方發出的。
  - 完整性：確保訊息在傳輸過程中未被篡改。

SNMP問題

- Community String 的安全性問題：
  - SNMP版本1和2c使用所謂的"community string"來控制對網絡設備的訪問權限，類似於密碼。"public"是最常見的預設讀取權限community string，而"private"用於讀寫權限。使用預設或弱的community string容易被猜測，從而導致未授權訪問。
- 明文傳輸的資訊：
  - SNMP v1和v2c在網絡上以明文形式傳輸資料，包括community strings。這使得傳輸的數據容易被截取和閱讀，進而泄露敏感信息。
- SNMP版本的選擇：
  - SNMP v3提供了比v1和v2c更強的安全功能，包括訊息加密、身份驗證和訊息完整性檢查。不過，並非所有設備都支援v3，且配置和管理v3比前兩個版本更複雜。

IOC、TTPS、IOA

- TTPS：指戰術、技術與程序，這些概念被廣泛應用於網絡安全領域，用以描述攻擊者的行為模式和操作方法。
- 正在被入侵（IOA, Indicators of Attack）：當你發現一些跡象或事件，這些可能表明有人正在嘗試入侵你的系統。這些跡象可能包括：
  - 系統或網絡中出現異常的流量模式，比如突然的流量增加或來自不尋常地理位置的訪問。
  - 大量的登錄失敗嘗試，可能表明有人在嘗試破解密碼。
  - 系統上出現未授權或未知的進程和服務，可能是攻擊者試圖控制系統。
  - 網絡設備上異常的端口掃描活動，表明有人在尋找系統弱點。
- 已經被入侵（IOC, Indicators of Compromise）：當你發現一些跡象或事件，這些表明你的系統已經被成功入侵。這些跡象可能包括：
  - 發現與已知惡意軟體或勒索軟體相匹配的檔案或hash值。
  - 系統文件或配置被未授權修改。
  - 敏感資料被未授權訪問或竊取，比如日誌文件顯示不尋常的數據傳輸。
  - 出現異常的用戶帳戶行為，如未授權的用戶帳戶創建或權限提升。

安全軟體發展生命週期

- 安全軟體發展生命週期(Security Software Development Lifecycle, SSDLC)：是一個將安全性整合到軟體開發生命週期（SDLC）各階段的方法。其目的是確保在軟體開發的每一步都考慮到安全性，從而降低軟體中安全漏洞的風險，並提升軟體的整體安全性能。
  - 需求階段：確定安全需求和目標，並將其作為功能需求的一部分。
  - 設計階段：採用安全設計原則，進行威脅建模，以識別潛在的安全風險，並設計以防範這些風險。
  - 開發實作階段：開發過程中應用安全編碼標準和最佳實踐，進行代碼審查以識別安全問題。
  - 測試階段：進行安全測試，包括靜態應用程序安全測試（SAST）、動態應用程序安全測試（DAST）、軟體成分分析（SCA）等，以發現和修復安全漏洞。
  - 部署維運階段：在生產環境中實施安全配置，並進行持續的安全監控和更新，以應對新出現的威脅。

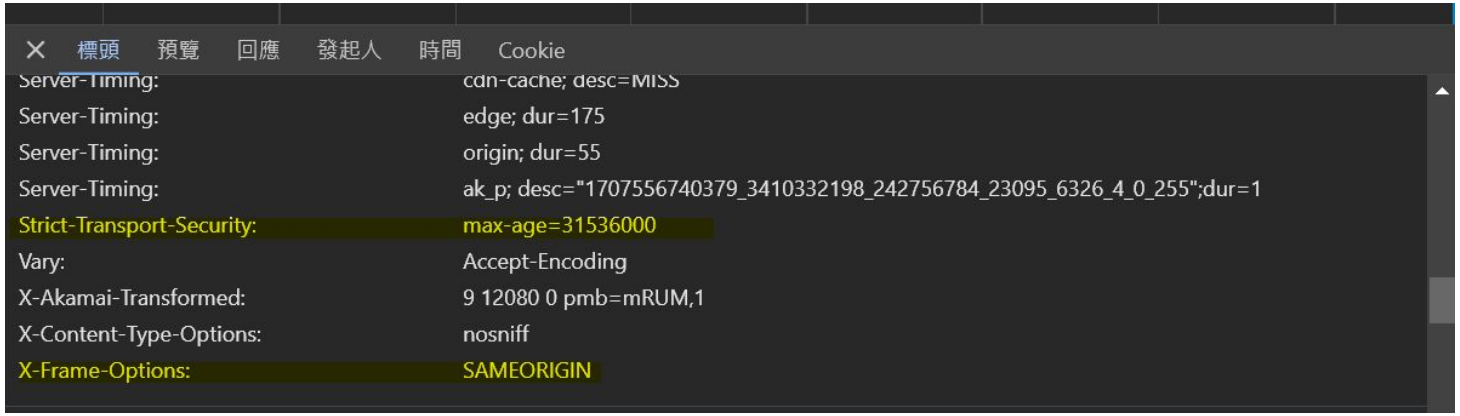
編碼、加密和雜湊

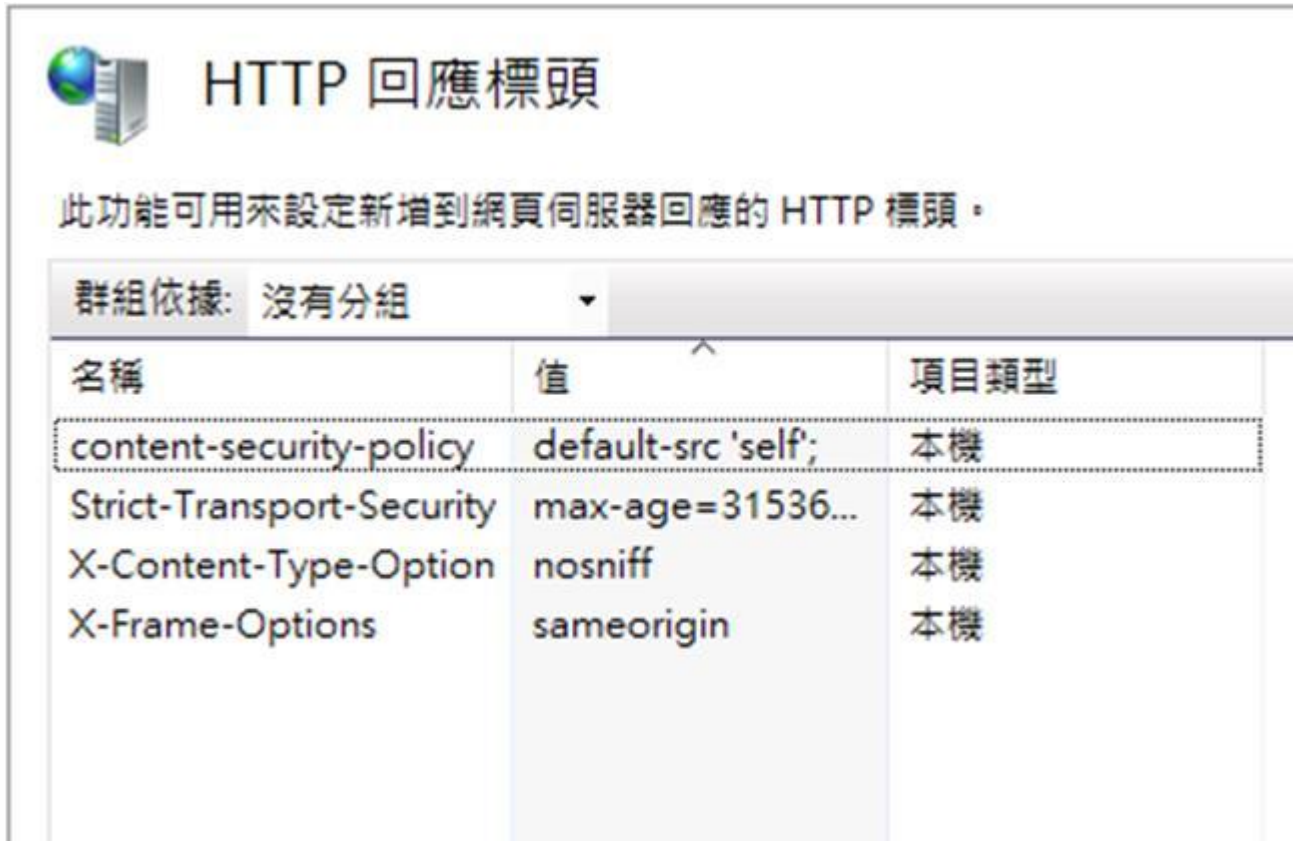
特性	編碼 (Encoding)	加密 (Encryption)	雜湊 (Hashing)
目的	轉換資料格式以便於傳輸或存儲	保護資料不被未授權的第三方讀取	確保資料的完整性和一致性
可逆性	可逆，通過公開的方法可以還原原始資料	可逆，但需要正確的密鑰	不可逆，不能從雜湊值還原原始數據
特點	資料轉換明確，經常用於資料的顯示或處理	需要密鑰來加密和解密資料	產生固定大小的雜湊值
常見算法	BASE 64、URL編碼	AES 128、RSA	SHA-256
應用場景	資料傳輸，如Email、XML/JSON資料處理	資料傳輸安全，如HTTPS、SSH	密碼儲存、資料校驗

HTTP Header 安全設定

- HTTP Strict Transport Security (HSTS)：強制客戶端（如瀏覽器）使用HTTPS與伺服器建立連線。

- X-Frame-Options：這個HTTP回應頭可以用來控制網頁是否允許被嵌入到frame、iframe或object。





XSS類型

- 反射式（Reflective）
  - 當使用者點擊包含惡意腳本的特製連結時觸發。腳本在使用者的請求發送到伺服器後，隨即由伺服器返回並在使用者的瀏覽器中執行。**攻擊是一次性的**，只有當用戶實際點擊連結時才會發生，**不儲存在網站上**。
- 儲存型（Stored）
  - 當攻擊者將惡意腳本儲存於網站上時觸發，例如在評論或留言板中。每當該頁面被瀏覽時都會執行。攻擊可以持續很長時間，影響所有瀏覽該頁面的使用者，**因此通常會儲存在資料庫裡**。
- 檔案物件模型（Document Object Model）
  - 當網頁的 JavaScript 錯誤地處理了用戶的輸入，並將其添加到 DOM 中時觸發。這種攻擊完全在客戶端發生，**惡意腳本由瀏覽器執行，而不是由伺服器返回**。攻擊依賴於用戶與網頁的互動。
- https://hackmd.io/yVOX8uJUTuCmfJccGD6dqw

備份 3-2-1原則

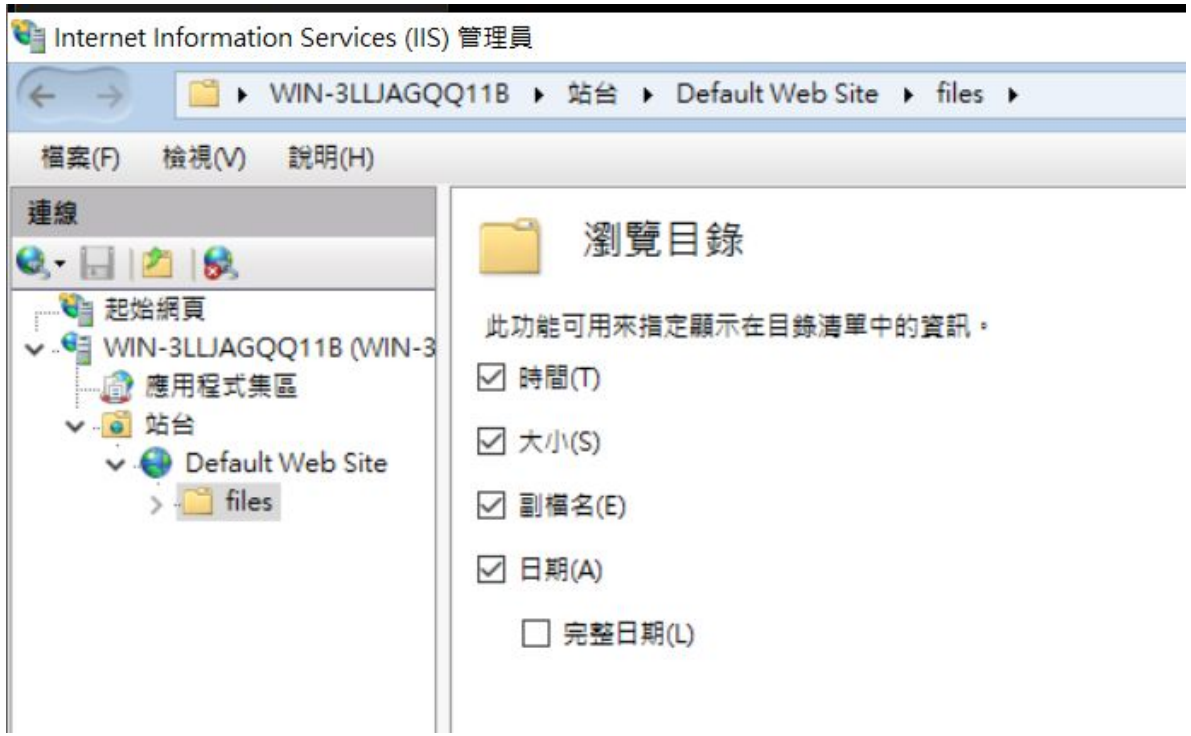
- 3份資料副本：保留原始資料以及兩份備份，這樣即便原始資料丟失或損壞，你也擁有兩份備份可以恢復。
- 2種不同的媒介：不要將所有備份保存在同一種類型的儲存媒體上。例如，你可以將一份備份保存在內部硬碟上，另一份保存在外部硬碟或雲端儲存上。這樣做可以防範特定儲存媒介故障的風險。
- 1份離線或離站的備份：至少有一份備份應該是離線的（即不連接到你的網絡或系統，從而避免網絡攻擊如勒索軟體的影響）或離站的（儲存在不同的地理位置，以防災難性事件如火災或洪水，影響到你的所有備份）。

SLA一年可停機的時間

- 越往下走停機時間越短
- 但是營運成本越高

SLA	一年可停機的時間
99%可用性	3.65天
99.9%可用性	8.76小時
99.99%可用性	52.56分鐘
99.999%可用性	5.26分鐘
99.9999%可用性	32秒

站台目錄列表（Directory Listing）漏洞



Tor（The Onion Router）網路

- Tor（The Onion Router）網路由美國海軍研究實驗室與其他研究機構合作開發，旨在確保政府通訊的安全。例如，為了使美國情報人員能在國外如俄羅斯安全地傳送資料，Tor被設計來提升通信的匿名性。
- 此外，鼓勵大眾使用Tor是為了使其流量混入普通網路活動中，從而不顯眼，尤其是在那些封鎖資訊的國家如中國和北韓，甚至有像CNN這樣的組織設立網站和提交文章，以規避如網絡長城之類的審查制度。
- Tor提供了一個使用者能夠在保持匿名的同時瀏覽網路的機制，從而增強了個人隱私和自由表達。儘管Tor網絡確實可用於訪問暗網並可能涉及非法活動，它同時也是許多尋求隱私保護和希望繞過網絡審查的人士的關鍵工具。