Port	協定/名稱	說明
20	ftp-data	FTP 資料連接埠
21	ftp	檔案傳輸協定 (FTP)
22	ssh	Secure Shell (SSH) 安全遠端連線服務
23	telnet	Telnet 遠端命令列連線服務
25	smtp	簡單郵件傳輸協定 (SMTP)
53	domain	網域名稱服務 (DNS)
69	tftp	簡易檔案傳輸協定，類似 FTP，由 Cisco 提出
80	http	網頁服務 (HTTP)
110	pop3	郵件接收協定 (POP3)
115	sftp	安全檔案傳輸協定 (SFTP)
123	ntp	網路時間同步協定 (NTP)
138	netbios-dgm	NETBIOS 資料包服務
139	netbios-ssn	NETBIOS 工作階段服務
143	imap	網際網路郵件存取協定 (IMAP)
443	https	安全網頁服務 (HTTPS)
445	microsoft-ds	微軟 SMB 服務（檔案分享）
1433	ms-sql-s	Microsoft SQL Server 資料庫
3306	mysql	MySQL 資料庫服務
3389	rdp	遠端桌面連線 (Remote Desktop Protocol)
8080	http	常用於替代 Port 80，或作為 Web Proxy
8443	https	常用於替代 Port 443，SSL 加密的 Web 服務

- 例如，Key=2, plain text為meet me after the toga party

```
m e m a t r h t g p r y
  e t e f e t e o a a t
```

- 得到密文為mematrhtgpryetefeteoaat

- 例如，Key=3, plain text為HELLOWORLD

```
H   O   L
  E L W R D
    L   O
```

- 得到密文為HOLELWRDLO

五種安全弱點的運作/利用方式：

1. **暴力破解（Brute Force）**
   - 攻擊密碼機制
   - 演算法弱點
   - 實體入侵破壞
   - 通行碼/密碼破解
     - 窮舉法：猜測所有組合
     - 字典攻擊

安全服務	說明
機密性	防止未授權者存取
完整性	確保資料未被竄改
可說明性	驗證資料來源與防止否認
鑑別性	確認身分是否屬實
不可否認性	確保發送者不能否認行為
可用性	確保資訊系統持續可使用

2. **資源耗盡（Resource Exhausting）**
   透過大量請求或操作使目標系統耗盡 CPU、記憶體、頻寬或儲存空間，造成系統延遲或癱瘓。
   - DoS, SYN Flood

3. **緩衝區溢位（Buffer Overflow）**
   將超出預期長度的輸入寫入緩衝區，進而覆蓋程式控制流程的資料（如返回位址），達到執行惡意程式碼的目的。

4. **格式字串（Format String）**
   攻擊者輸入特製格式字串（如 `%x %n`）被當成格式參數執行，可能洩漏記憶體資料或修改資料，造成任意程式碼執行。
   - SQL injection, XSS

5. **社交工程（Social Engineering）**
   透過心理操控誘騙使用者洩漏機密資訊，如釣魚網站、冒充信件或假冒技術支援等手法，繞過技術防線。

CVE vs CVSS

CVE（Common Vulnerabilities and Exposures，通用漏洞與曝險）是由 MITRE Corporation 管理的全球性漏洞編號系統，每個已知的安全漏洞都會被賦予一個唯一的 CVE 編號。

CVSS 則是用來評估這些 CVE 所代表漏洞的嚴重程度。例如，CVE-2021-44228（Log4j 漏洞）就被評為 CVSS 分數 10.0，表示其風險極高。

CVSS 的評分架構

CVSS 的評分範圍從 0.0（無風險）至 10.0（極高風險），並依據以下四大指標群組進行評估：

1. **基礎指標（Base Metrics）**：評估漏洞的固有特性，如攻擊向量（AV）、攻擊複雜度（AC）、所需權限（PR）、使用者互動（UI）、影響範圍（Scope）、機密性影響（C）、完整性影響（I）和可用性影響（A）。
2. **時間指標（Temporal Metrics）**：考量漏洞隨時間變化的特性，例如漏洞利用代碼的成熟度、修補措施的可用性和報告的可信度。
3. **環境指標（Environmental Metrics）**：根據特定組織的環境，評估漏洞對其資產的實際影響，並調整基礎分數以反映真實風險。
4. **補充指標（Supplemental Metrics）**：在 CVSS 4.0 中新增，用於補充其他未涵蓋的風險評估因素。

DNS RR type

SOA
- Start Of Authority，網域管理資訊

NS : name server
- DNS伺服器主機名稱

A/AAAA : IPv4 / IPv6 Address
- DNS網域名稱 對應到IPv4 / IPv6 Address

CNAME : canonical name
- 主機名字的別名

MX : mail exchanger
- 郵件傳輸代理（MTA, Message Transfer Agents）

PTR : pointer
- IP 對應的 domain name

TXT : 任意可讀的文字

```
          ↓
金鑰: 4 3 1 2 5 6 7
明文: a t t a c k p
      o s t p o n e
      d u n t i l t
      w o a m x y z
```

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

DNS Zone Transfer

DNS Zone Transfer 是什麼？

DNS Zone Transfer（區域轉移） 是 DNS 伺服器之間用來同步 DNS 記錄的一種機制，主要用於主從 DNS 之間的備援與更新。

核心概念

- 企業常自建多台 DNS 伺服器（主伺服器 + 備援伺服器）
- 為保持 DNS 資料一致，會啟用 Zone Transfer 功能
- 透過 `AXFR` 協定讓一台 DNS Server 取得另一台的完整 zone 記錄

安全風險 ...

工具示範

使用 `dig` 或 nslookup 搭配 `axfr`：

```
dig axfr zonetransfer.me @nsztm1.digi.ninja
```

或在 Windows 下使用：

```
[[nslookup]]
server nsztm1.digi.ninja
ls -d zonetransfer.me
```

線上工具： ...

防護建議

在 DNS 設定檔（如 `/etc/named.conf`）中**限制允許 zone transfer 的 IP 清單**

```
options {
    allow-transfer { 1.2.3.4; 5.6.7.8; };
};
```

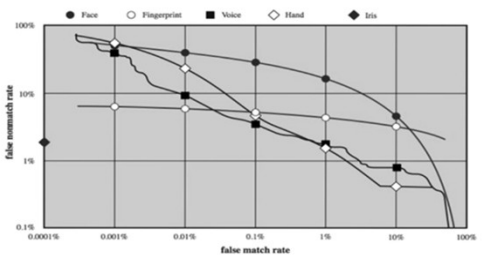
- 常利用XOR運算作加/解密，以明文HELLO，KEY為APPLE，轉為ASCII後加密如下

Key	A 01000001	P 01010000	P 01010000	L 01001100	E 01000101
原文	H 01001000	E 01000101	L 01001100	L 01001100	O 01001111
加密	00001001	00010101	00011100	00000000	00001010

生物特徵認證

技術	說明	標準
指紋	快速、正確性高	ISO/IEC JTC 1/SC 37 19794-2
指靜脈	不可複製，適用高安全環境	
人臉／虹膜	非接觸式，適合公共空間	ISO/IEC JTC 1/SC 37 19794-5

- 評估指標：
  - FMR（False Match Rate 錯誤接受率）
    - 將不合法誤判為合法
  - FNMR（False Non-Match Rate 錯誤拒絕率）
    - 將合法誤判為不合法
  - Decision Threshold（需調整以達成平衡）



事件 ID	說明
1102	清除安全日誌
4624	登入成功
4625	登入失敗
4634	登出
4768	請求 kerberos 驗證
4688	建立新行程
4689	結束行程
4771	kerberos驗證失敗
7045	新服務被安裝
7045	系統安裝新服務

分數範圍	嚴重程度
0.1–3.9	Low
4.0–6.9	Medium
7.0–8.9	High
9.0–10.0	Critical

```c
#include <stdio.h>
#include <string.h>

// ！這是目標函式，利用者攻擊後希望讓程式執行到這裡！
void secret_function() {
    printf("Hacked! You got into the secret function!\n");
    fflush(stdout);
}

// 這是含有 buffer overflow 弱點的函式
void vulnerable_function() {
    char buffer[10];

    printf("Enter some text: ");
    fflush(stdout);

    // 這裡是程式的漏洞：
    // gets() 會從 stdin 讀取使用者輸入，直到換行符為止，
    // 但它不會檢查 buffer 大小，可能造成「緩衝區溢出」
    gets(buffer);

    printf("You entered: %s\n", buffer);
}

int main() {
    vulnerable_function();
    printf("Program finished.\n");
    return 0;
}
```

欄位名稱	說明與範例
網域名稱	這條SOA記錄所屬的網域：`zonetransfer.me.`
TTL	存活時間 (Time to Live)：`7200`
Class	記錄類型，IN代表Internet：`IN`
Record Type	記錄型態，SOA代表Start of Authority：`SOA`
Primary NS	主要DNS伺服器：`nsztm1.digi.ninja.`
Admin Email	管理員信箱（@變成.）：`robin.digi.ninja.`
Serial Number	區域檔版本號：`2019100801`
Refresh	次要DNS多久要向主要DNS重新抓取：`172800`
Retry	抓取失敗後，多久要重試：`900`
Expire	次要DNS最多可容忍多久沒成功更新：`1209600`
Minimum TTL	最小存活時間，控制NXDOMAIN等快取時間：`3600`

zonetransfer.me. 7200 IN SOA nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209600 3600

ex:

`zonetransfer.me. 7200 IN MX 0 ASPMX.L.GOOGLE.COM.`

欄位名稱	說明與範例
網域名稱	這條MX記錄所屬的網域：`zonetransfer.me.`
TTL	存活時間 (Time to Live)：`7200`
Class	記錄類型，IN代表Internet：`IN`
Record Type	記錄型態，MX代表Mail Exchange：`MX`
優先順序	郵件伺服器的優先順序，數字越小越優先：`0`
郵件伺服器	處理這個網域的郵件伺服器：`ASPMX.L.GOOGLE.COM.`

zonetransfer.me. 7200 IN MX 0 ASPMX.L.GOOGLE.COM.

TCP 連線狀態	說明
LISTEN	等待來自遠端 TCP 應用程式的連接請求
SYN-SENT	發送連線請求（SYN）後，等待遠端確認（三向交握第 1 步）
SYN-RECEIVED	收到 SYN 後送出 SYN+ACK，等待對方回應（三向交握第 2 步）
ESTABLISHED	三向交握完成，建立連線，可開始資料傳輸
FIN-WAIT-1	等待連線關閉狀態，等待確認終止請求或遠端同時終止
FIN-WAIT-2	等待遠端的連接終止請求（已送出自己的終止請求）
CLOSE-WAIT	收到終止請求後，等待本地應用程式處理關閉
CLOSING	雙方幾乎同時發送終止請求，等待遠端確認
LAST-ACK	發送終止請求後，等待遠端確認
TIME-WAIT	等待一段時間，保證遠端有收到自己的終止請求
CLOSED	連線完全關閉，釋放資源

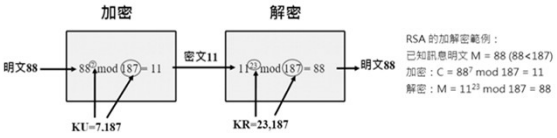
標準Feistel區塊加密特性

- 區段大小(block size)
  - 增大區段可以提升安全性，但是加解密會變慢
- 金鑰長度(key size)
  - 增加長度可以提升安全性，使得暴力搜尋金鑰變得更困難，但是加解密會變慢
- 回合數(number of rounds)
  - 增加回合數可以提升安全性，但是加解密會變慢
- 子金鑰的產生(subkey generation)
  - 複雜的產生方法可以使分析變困難，但是加解密會變慢
- 回合函式(round function)
  - 複雜的函式可以使分析變困難，但是加解密會變慢

類型	名稱	特性	狀態
對稱	DES	舊、56-bit、易被破解	⛔ 不建議
對稱	3DES	DES 加強版	⚠ 可接受但慢
對稱	AES	128/192/256-bit 安全	☑ 首選
非對稱	RSA	基於大數分解難度	☑ 廣泛應用
非對稱	ECC	相同安全等級下金鑰更短	☑ 手機/IoT 常用
雜湊	MD5、SHA-1	已遭碰撞	✖ 停用
雜湊	SHA-2、SHA-3	安全	☑ 推薦

RSA範例(1)

1. 選取質數： p=17 與 q=11
2. 計算N= pq =17×11=187
3. 計算φ(N)=(p–1)(q-1)=16×10=160
4. 選取e使得 gcd(e,160)=1; 選取 e=7
5. 求取d 使得 de=1 mod 160 且 d < 160；其值為 d=23 因為 23×7=161= 1×160+1
6. 發佈公開金鑰 KU={7,187}
7. 保存秘密私密金鑰 KR={23, 187}



RSA 的加解密範例：
已知訊息明文 M = 88 (88<187)
加密：$C = 88^{7} \bmod 187 = 11$
解密：$M = 11^{23} \bmod 187 = 88$

Google Hacking

指令	功能
`inurl:`	網址中包含關鍵字
`intitle:`	標題包含關鍵字
`intext:`	正文內容包含關鍵字
`filetype:`	搜尋特定檔案類型
`site:`	限定網站範圍
`link:`	找出連結到該網站的 URL

OS Fingerprint

利用各種作業系統版本對收到的封包所產生的不同回應封包內容，可用來區分辨識作業系統的類型或版本。

Nmap ...

常見技術

- TCP FIN flag偵測：檢測對未開 port 的回應方式
- BOGUS flag偵測/偽造flag偵測：發送異常 TCP flag 封包觀察反應
- TCP ISN Sampling：看初始序號變化
- ICMP error Message Quenching：比對錯誤訊息的速率與回應