

國立臺灣師範大學資訊工程學系個人申請： 資安組試題範本

共 13 題

考試時間：10:30-12:00

滿分總共 130 分。「資訊安全」是一門很麻煩的科目，要保護「資訊系統」的安全，前提是你要先了解「資訊系統」，也就是泛指「所有」資工系的課程。坦白說這是很困難的，畢竟人一天就 24 小時，因此你如果只會部份的題目「這很正常」。你不會別人也不一定會，請放輕鬆、保持愉快的心來作答。

1 程式設計

1. (10 points) 請問下面程式碼的輸出是？

```
1 #include <stdio.h>
2
3 int main()
4 {
5     int ans = 0;
6     for( int i = 0, j = 0 ; i < 5 ; j = j + (i++) )
7     {
8         ans += j;
9     }
10    printf( "%d\n", ans );
11    return 0;
12 }
```

2. (10 points) 請問下面程式碼的輸出是？

```
1 #include <stdio.h>
2
3 int f( int x, int y )
4 {
5     if( y == 0 ) return 1;
6     if( y % 2 == 0 )
7     {
8         int ret = f( x, y >> 1 );
9         return ret * ret;
10    }
11    else
12    {
```

```

13     int ret = f( x, y >> 1 );
14     return ret * ret * x;
15 }
16 }
17
18 int main()
19 {
20     printf( "%d\n", f(2,7) );
21     return 0;
22 }

```

3. (10 points) 在 C 語言中，同學們應該習慣使用 **scanf** 以及 **%d** 去取得使用者輸入的整數。請看看下面這隻程式，如果我們使用 **%s** 去取得使用者輸入的字串，請問這個寫法會有什麼潛在的問題呢？

```

1 #include <stdio.h>
2
3 int main()
4 {
5     char str[16] = {0};
6
7     scanf( "%s", str );
8
9     return 0;
10 }

```

2 系統安全

1. (10 points) 請看看下面 shell 指令的執行結果。

```

1 $ ls -l /etc/passwd
2 -rw-r--r-- 1 root root 2145 10月  4 15:13 /etc/passwd

```

請解釋 **-rw-r--r-- 1 root root** 的意義。

2. (10 points) 在 Linux 的系統中，使用者的密碼過去是存在 **/etc/passwd**，後來則是存在 **/etc/shadow**。請問密碼在這兩個地方的儲存方式有什麼不同呢？
3. (10 points) 請解釋下面這行指令的意義。

```

1 $ sudo dd if=/dev/hda of=~/.hdadisk.img

```

3 網路安全

1. (10 points) **tracert** 是一種電腦網路工具，它可顯示封包在 IP 網路經過的路由器的 IP 位址。請簡單描述 **tracert** 的運作原理。

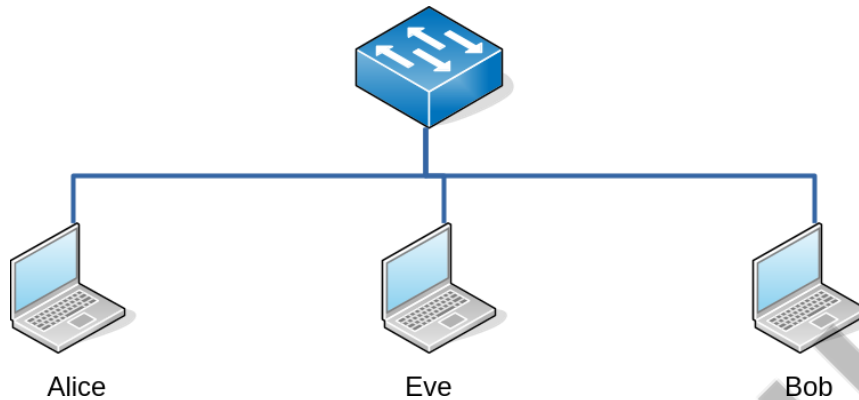


Figure 1: 該如何發動中間人攻擊呢？

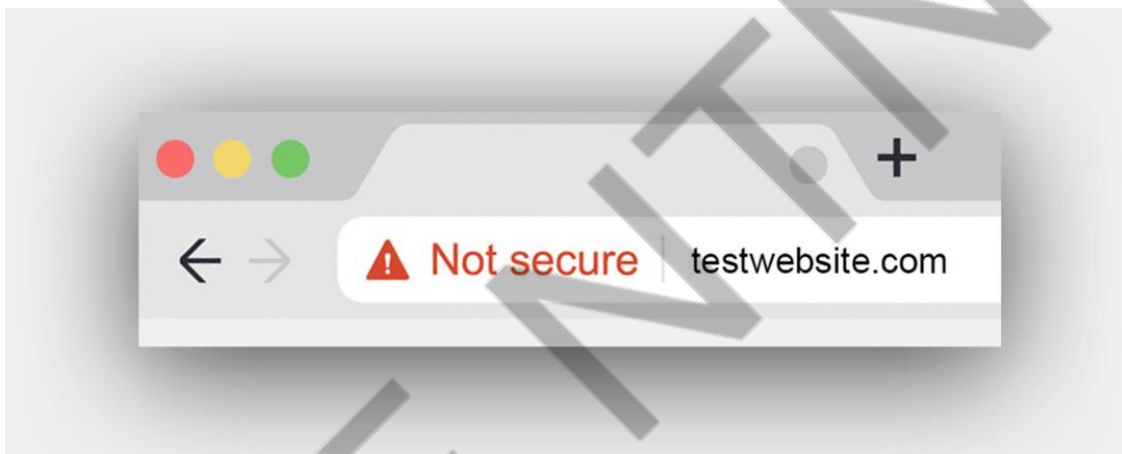


Figure 2: Not secure warning on the browser.

2. (10 points) 中間人攻擊（英語：Man-in-the-middle attack，縮寫：MITM）在密碼學和電腦安全領域中是指攻擊者與通訊的兩端分別建立獨立的聯絡，並交換其所收到的資料，使通訊的兩端認為他們正在通過一個私密的連接與對方直接對話，但事實上整個對談都被攻擊者完全控制。給一個區域網路的拓樸如圖 1 所示，請寫出如何讓 Eve 去發動中間人攻擊，竊聽 Alice 和 Bob 中間的通訊。
3. (10 points) 網域名稱系統（英語：Domain Name System，縮寫：DNS）是網際網路的一項服務。請簡介它的運作原理。
4. (10 points) 當我們用瀏覽器去瀏覽某些網站的時候，會看到如圖 2 的畫面，請寫出至少三個可能的理由。

4 密碼學

1. (10 points) 下面這段密文是以凱撒加密法進行加密的，請將它還原成原本的信息。

Jwm anvvnkna, cqn cadcq cqjc xwln fjb byxtnw: Cx uxen jwxcqna ynabxw
rb cx bnn cqn ojln xo Pxm.

2. (10 points) 請計算 2^{1234} 除以 13 的餘數。
3. (10 points) 很多網站在要求使用者輸入密碼時，會要求「最小密碼長度必須大於特定值」以及「必須包含特殊符號」。請比較這兩個措施，哪一個對於密碼強度的提昇比較有幫助？