# 資訊安全相關重要知識

```

1.Hacker 相關知識

1.1Hacker

1.2Cracker

1.3 Script Kiddie

1.4駭客需要精通的基礎

1.5駭客入侵或攻擊的方法

1.6駭客具備的特殊網路環境及網路安全知識

1.7駭客分類

2.網路封包分析工具

2.1wireshark

```

## 1. Hacker 相關知識

### 1.1 Hacker

```

1.一個對某領域程式語言有足夠了解,可以不經長時間思考就能創造出有用的軟體的人。

2.喜愛程式設計(Coding)並享受在其中,變得更擅長於程式設計的人。

3.喜愛自由(Freedom),不易受約束,但覺得假如是為了喜愛的事物,可以被受適當的約束。

4.一個試圖破解某系統或網路以提醒該系統所有者的電腦安全漏洞。

這群人往往被稱做「白帽黑客」(sneaker)」。

許多這樣的人是電腦安全公司的僱員,並在完全合法的情況下攻擊某系統。

Hacker是一個透過知識或猜測而對某段程式做出(往往是好的)修改,並改變(或增強)該程式用途的人。

```

### 1.2 Cracker

```

「黑客、怪客」(cracker):一個惡意(一般是非法地)試圖破解或破壞某個程式、

系統及網路安全的人。

簡體字地區,稱為「駭客」(cracker),繁體字稱黑客(黑帽駭客)、怪客、垮客等。

「cracker」不同於「Hacker」。

「cracker」没有「Hacker」精神,也沒有道德標準。

「Hacker」們建設,而「cracker」們破壞。

```

### 1.3 Script Kiddie

```

「脚本小子」則指那些完全没有或僅有一點點駭客技巧,而只是按照指示或執行某種駭客程式來達到破解目的的人。

腳本小子是利用他人所編輯的程式來發起網路攻擊的網路鬧事者,他們通常不懂得攻擊物件的設計和攻擊程式的原理,

不能自己偵錯系統發現漏洞,實際職業知識遠遠不如他們通常冒充的黑帽駭客。

不少青少年因為網路入侵,傳播病毒木馬偷竊獲利,破壞報復攻擊等原因而犯上電腦犯罪,

```

### 1.4駭客需要精通的基礎

```

1,數學和英語,網際網路70%都是英文網站,非常多的資源都是英語撰寫的。

2,網路/作業系統,精通網路如TCPP以及網路原理,才能成為一名「硬體型駭客」。

而對作業系統的熟悉與精通,才能更深入去學習如何入侵以及發現當中的漏洞。

3,程式語言,必須精通組合話言、CC++、資料庫、SQL、網路程式設計。

4,對任何事查根究柢的好奇心與批判性的思考。

```

### 1.5駭客入侵或攻擊的方法

```

1,掃描(Scanning)和列舉(Enumeration )

2,判斷作業系統並發現漏洞

3,社交專案(Social Engineering )

4.提高在遠端作業系統的管理員許可權(Privilege Escalating ) o

5.口令攻擊,漏洞攻擊,緩衝蓖溢位攻擊,DDoS拒絕服務攻駛,欺騙類攻擊等

等。

```

### 1.6駭客具備的特殊網路環境及網路安全知識

```

1,資訊竊聽偵測以及連線劫持技術

2.非 Windows 作業系統以及無線網路安全攻防技術

3,密碼學以及密碼猜測和破解

4,熟練編寫木馬、后門、電腦病毒蠕蟲病毒並掌握其攻防原理,

5,針對防毒軟體、防火牆以及入侵偵測系統的技術,

6.對交換裝置的攻擊,需要駭客有一定的漏洞代碼缺陷發現能力。

```

### 1.7駭客分類

```

1.駭客

擁有熟練電腦技術的人，但大部分媒體將 駭客 用於電腦入侵者。

2.白帽駭客

有能力破壞電腦安全但不具備惡意的駭客。

白帽子通常有清楚的道德規範並常試圖與企業合作改善被發現的安全弱點。

3.灰帽駭客

對於倫理和法律曖昧不清的駭客。

4.黑帽駭客

犯罪與駭客的混成語

5.紅帽駭客

激進駭客(hackivist)或譯為 駭客活動分子、倡權駭客等，例如中國的紅客

```

## 2.網路封包分析工具

### 2.1wireshark

```

Wireshark(前稱 Ethereal)是一個網路封包分析軟體。

網路封包分析軟體的功能是截取網路封包,並盡可能顯示出最為詳細的網路封包資料。

在過去,網路封包分析軟體是非常昂貴,或是専門屬於營利用的軟體,Wireshark 的出現改變了這一切。

在 GNUGPL通用許可證的保障範圍底下,使用者可以以免費的代價取得軟體與其程式碼,並擁有針對其原始碼修改及客製化的權利。

以純文字傳輸密碼,容易讓密碼被網路封包分析軟體、封包竊聽器攔截。

網路竊聽器:指會執行擷取並分析網路通訊動作的軟體或硬體。

```