第九章

網頁密碼破解

認證（Authentication）

- 是用來識別使用者身分的流程，在私人或公共的電腦網路上，認證可以透過輸入帳號及密碼來完成。
- 認證成功代表使用者可以使用該系統，是不可缺少的步驟。
- 在各種的認證操作方式中，以網頁為基礎的認證最容易受到駭客的攻擊，因為網頁是經常性且公開的放在網路上供使用者存取，稍一不慎就會遭到入侵。

HTTP 認證

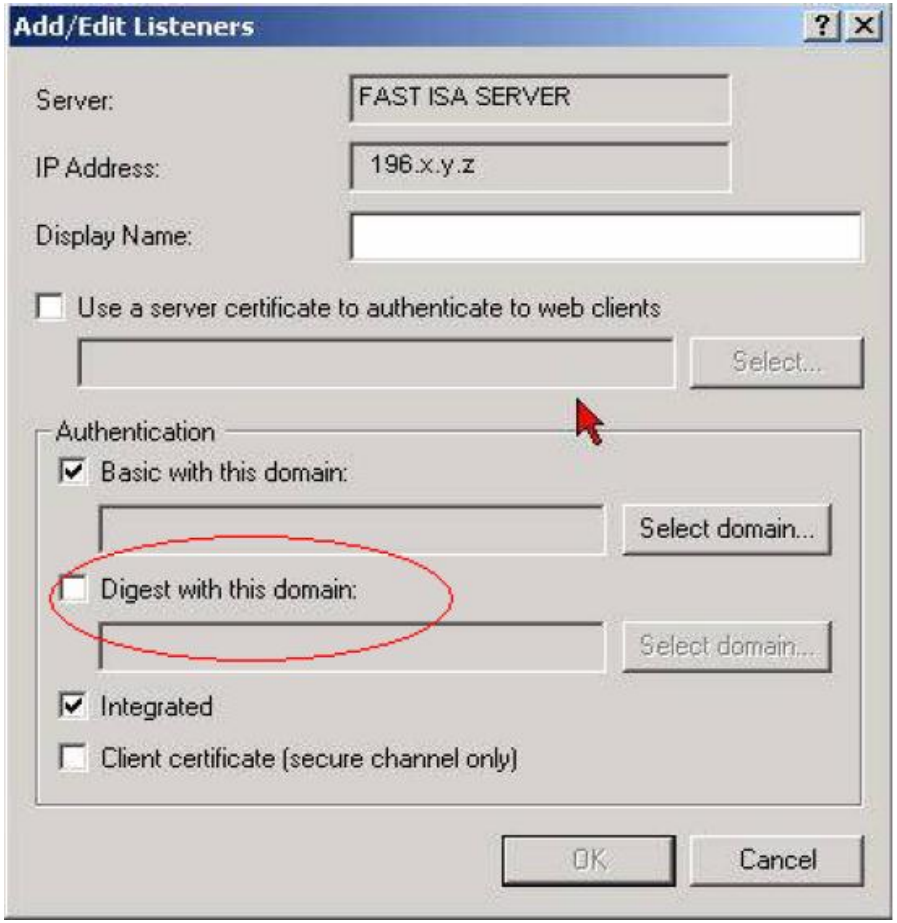
- 基本認證（Basic Authentication）
- 摘要認證（Digest Authentication）

基本認證

- 網頁應用程式最基本的驗證形式，因為帳號及密碼在傳送時並沒有加密，因此也最容易遭受攻擊及竊聽。

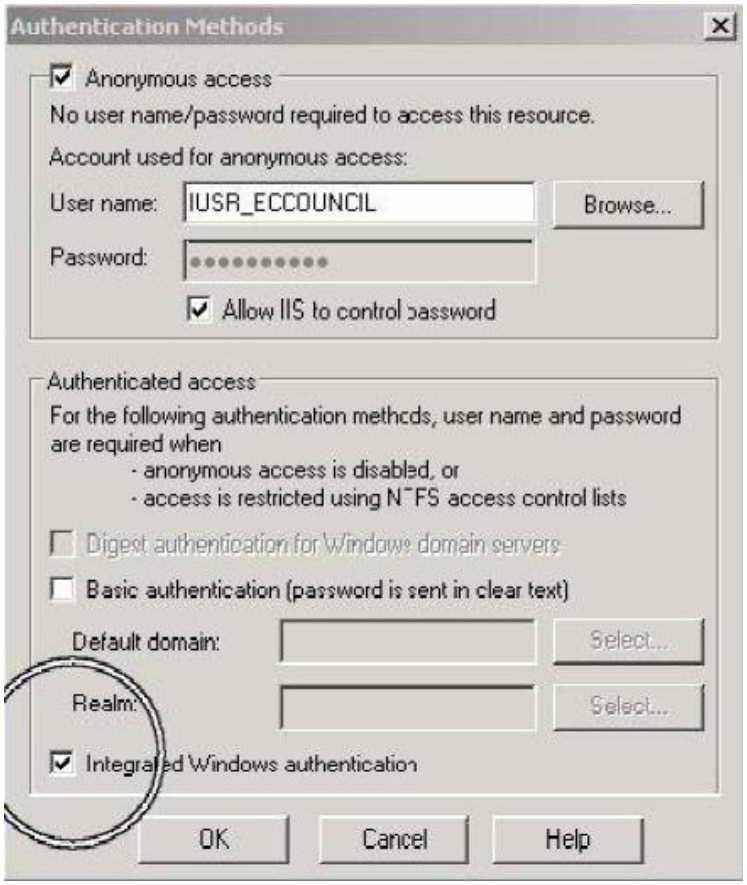
摘要驗證

- 基本方法和前述的「基本驗證」是一樣的，只是帳號和密碼在網路上傳送之前，會先將帳號及密碼予以加密 。



整合式視窗NTLM驗證

- 整合式視窗NTLM認證是在HTTP協定上，使用微軟特有的NT LAN Manager（NTLM）驗證程式，這種認證只工作於微軟的Internet Explorer瀏覽器及IIS網頁伺服器，不能在其他瀏覽器或伺服器上執行。



協商驗證

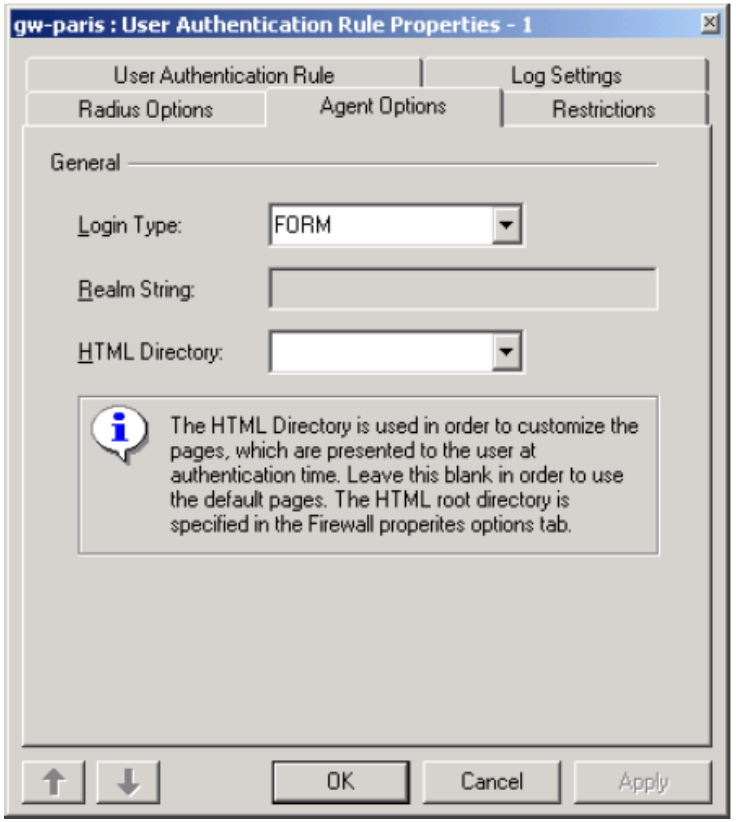
- 協商驗證（Negotiate Authentication）是將NTLM驗證功能進行延伸加強，在Windows 2003 Server中使用，能提供Kerberos-based驗證，它使用協商程序（negotiation process）去決定要使用的安全層級 。

憑證式認證

- 憑證式認證（Certificate-Based Authentication）使用x.509公鑰/私鑰加密法（Public/Private key cryptography）及數位憑證去認證使用者，此法很少有工具可以破解 。

表單式驗證

- 表單式驗證（Forms-Based Authentication）是Internet上最普遍的驗證技術，不需要依賴特殊的支援，是可以高度客制化的驗證機制，通常使用最基本的網頁協定 HTML 即可。



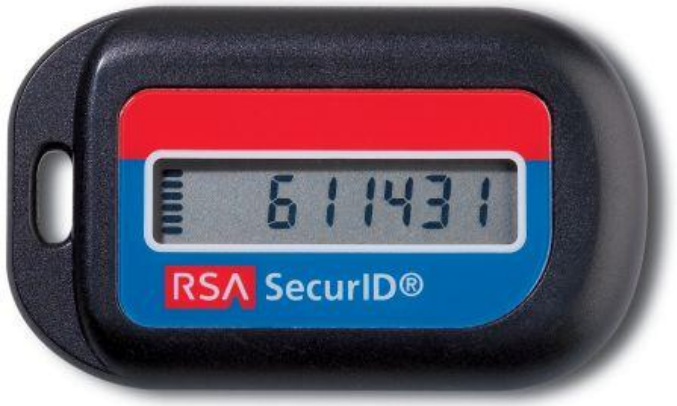
微軟護照驗證

- 單一簽入（Single sign-on）是讓使用者只要記住一組帳號密碼就可以在多個系統間使用。

- 微軟護照驗證（Microsoft Passport Authentication）是在Microsoft's universal single sign-in（SSI）平台上執行，它可以讓使用者用一組帳號密碼去存取任何使用微軟護照驗證的網站，例如MSN、Hotmail及MSN Messenger，微軟鼓勵其他的廠商也使用此平台。

輔助認證

- RSA SecurID Token認證方式包含了一個「物件」，它是一個硬體裝置，這個裝置有內建的時鐘及編碼，每隔若干時間會產生一個認證碼，使用者依據顯示的這組號碼，可以登入目標系統中。



生物識別技術

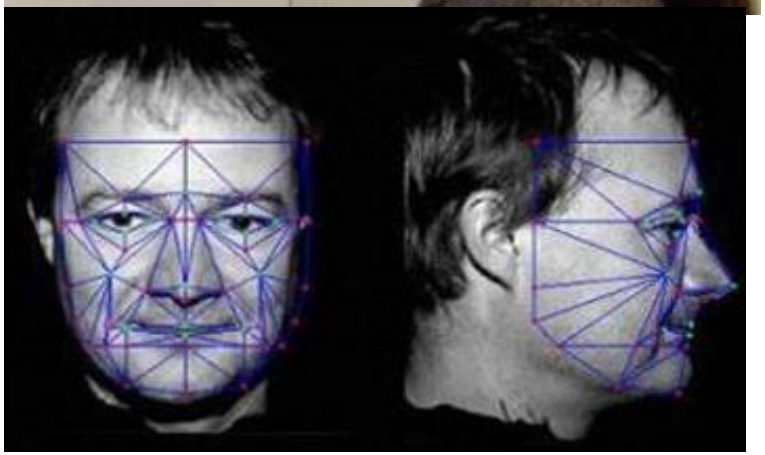
- 指紋辯識

- 手掌靜脈

生物識別技術

- 虹膜 識別

- 人臉識別



圖片式驗證碼

- 所謂圖片驗證碼，就是將一串隨機產生的數字或符號，利用程式轉換成圖片，圖片裏面可能還會加上一些干擾的圖素（防止辨識），必須由使用者用肉眼去識別其中的數字，並將其輸入表單中，然後由網站進行驗證，驗證成功後才能讓使用者使用 。

資料加密技術

- 網頁在傳送的過程中，很容易被竊聽，因此網頁的密碼或資料在傳送之前，可以先以資料加密技術進行演算，結果會得出一組無法直接辨識的數字，再將此數字進行傳輸，就可防止資料被監聽竊取 。

MD5加密

- MD5（message-digest algorithm）是由MIT的R. Rivest教授在1992年所提出的加密演算法，有下列優點：

1. 不可逆性（one way hash function）
2. 唯一性（database password check）
3. 濃縮訊息（message digest）
4. 數位簽章（digital signature）

SHA加密

- SHA1也是一種加密演算法，是由National Institute of Standards and Technology（NIST）在1994年改良也是由該組織所發展的SHA（the Secure Hash Algorithm）加密演算法而來 。

網頁密碼破解

- 網頁密碼破解者(Cracker) 使用下面方法得到密碼：

（1）偷取密碼。

（2）猜測密碼。

（3）暴力攻擊法（brute-force）。

（4）字典攻擊法（dictionary searches）

（5）混合型攻擊法（Hybrid。

密碼猜測

- 網頁密碼猜測可以使用手動或者是使用工具程式自動進行。

- 常用的密碼包括root、administrator、admin、operator、demo、test、webmaster、…。

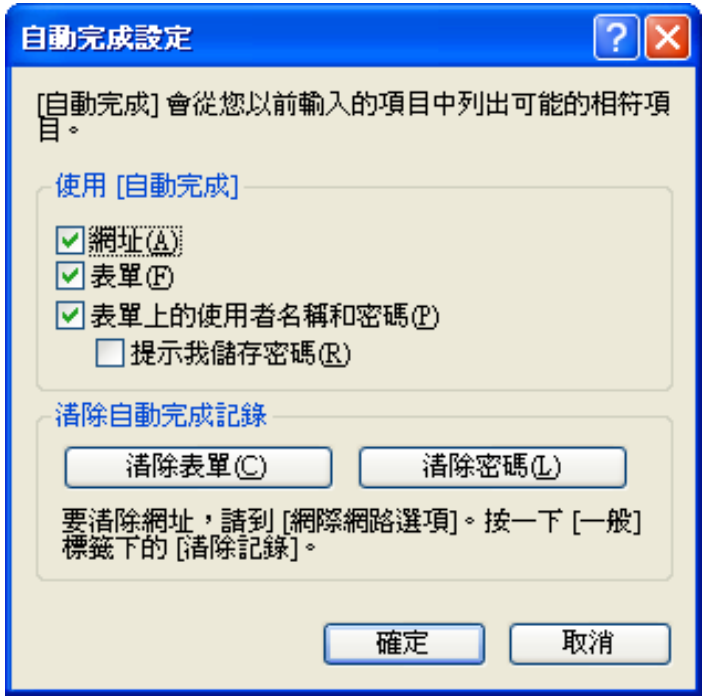
查詢字串

- 查詢字串是URL中在?後的額外資料位元，用來傳遞變數與值。這個查詢在client與server間傳輸資料。

http://www.mail.com/mail.asp?mailbox=sue&company=abc%20com

- 瀏覽器會將輸入的資料記錄起來，以備未來使用，同時瀏覽器可能有網址「自動完成」的功能，在輸入網址時，會將之前紀錄顯示出來提供參考。

- 但是這功能同時也很有可能會把在URL後面的密碼顯現出來



Cookies

- Cookies是網站伺服器（Web Server）儲存在使用者瀏覽器中的一部分資訊。當您瀏覽網站時，一些Cookies將被設定於瀏覽器內，使瀏覽器記下一些特定的資訊，以便網站伺服器在未來能夠更加方便被使用。

- 當關閉瀏覽器時，Cookies有些會立即隨之消失，有些就被儲存於電腦記憶體中的Cookies檔內。

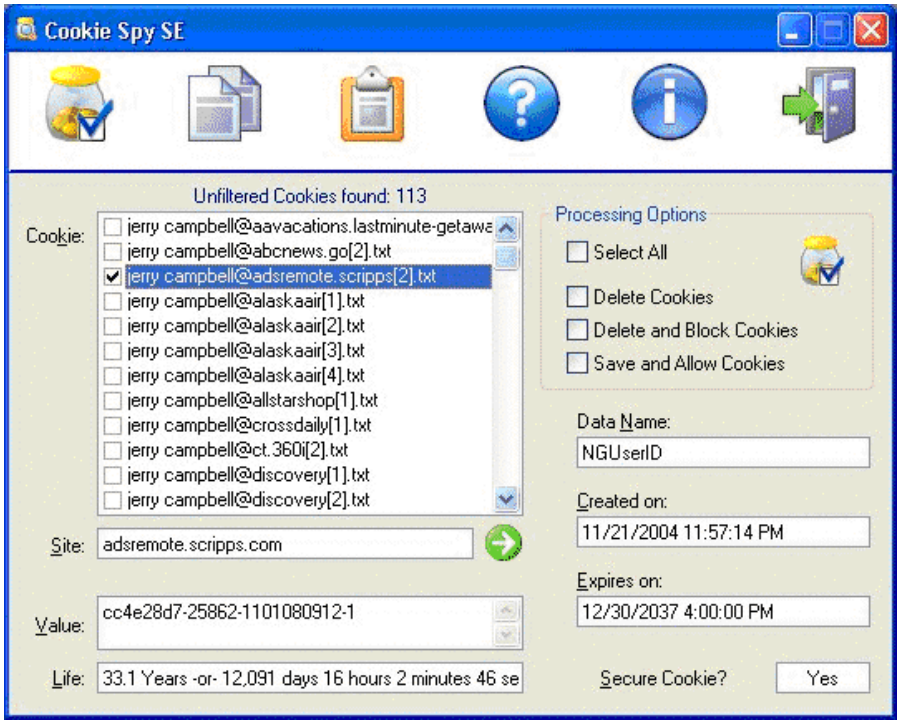
Cookies

- 所有的Cookies都有時效限制，時間到了就自動清除。
- Cookies是設定於特定電腦內的瀏覽器內，使用其他電腦連結相同網站伺服器時，Cookies將會重新被紀錄。
- Cookies常用來儲存表單中重要的欄位，例如：記錄帳號、使用者名稱...等。

工具程式

- **CookieSpy**

- 是管理Cookie重要的工具，可以將電腦中所有曾經儲存的Cookie列表出來，並決定要保留還是刪除。



對策

網頁密碼有以下的對策可以參考：

- 密碼最少必須八個字。
- 密碼字母必須是大小寫及特殊字（數字及符號）的組合。
- 字典中容易找到的字不能用來當作密碼。
- 不能用有關個人的公共資訊當作密碼。

對策

- 個人的資訊不能拿來當作密碼。
- 帳號名稱及密碼不能相同。
- 強密碼必須是建立於組織的安全政策當中。
- 系統管理者確認使用者是使用適當的強密碼。
- 安裝新系統必須確認立即改變預設的密碼。

對策

- 每隔一段時間改變密碼。
- 不要用郵件寄送密碼。
- 畫面上若詢問是否要儲存密碼？回答「否」。
- 不告訴任何人你的密碼。
- 使用圖片式驗證碼。

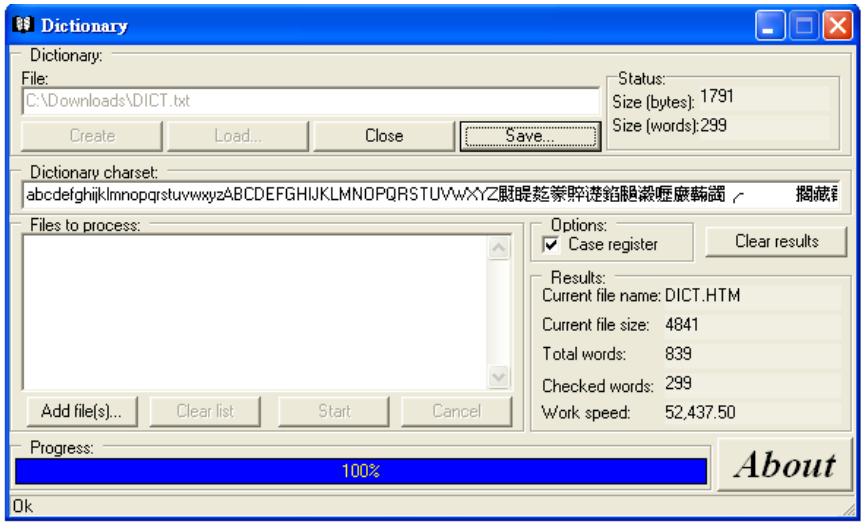
工具程式

- 可在網頁中加入檢驗密碼強度的簡易JavaScript程式，讓使用者在第一次輸入密碼或變更密碼時，都能依照強密碼的規則進行輸入 。

- http://www.dreamincode.net/code/snippet66.htm

工具程式

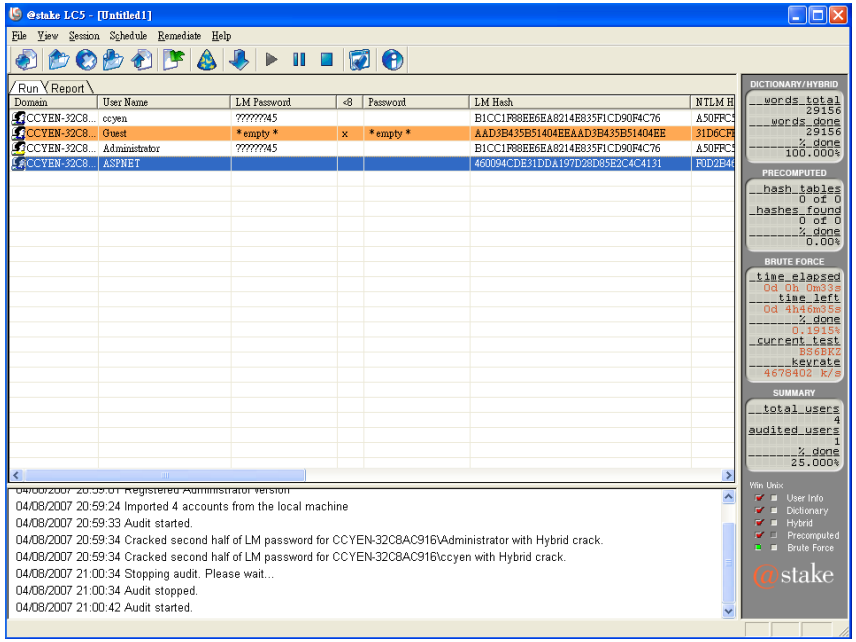
- Dictionary Maker
- 這個程式可以利用現成的文件來產生密碼檔。



工具程式

- LOphtcrack

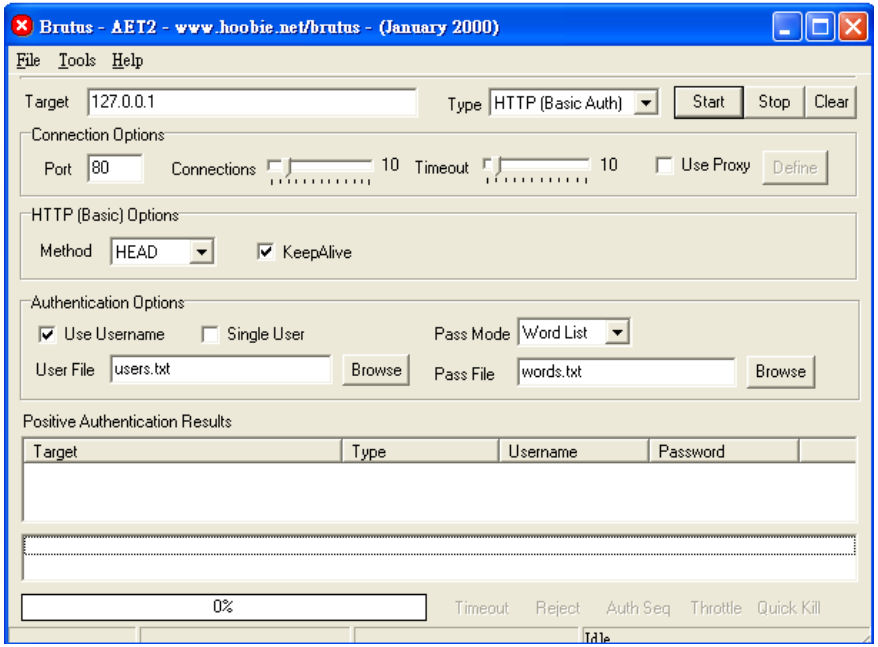
- L0phtCrack就是LC5，能試著從Hash表中破解Windows及UNIX密碼，也有多種方法產生密碼猜測（dictionary及brute force等），此外也可以監聽網路上的帳號進行密碼破解 。



工具程式

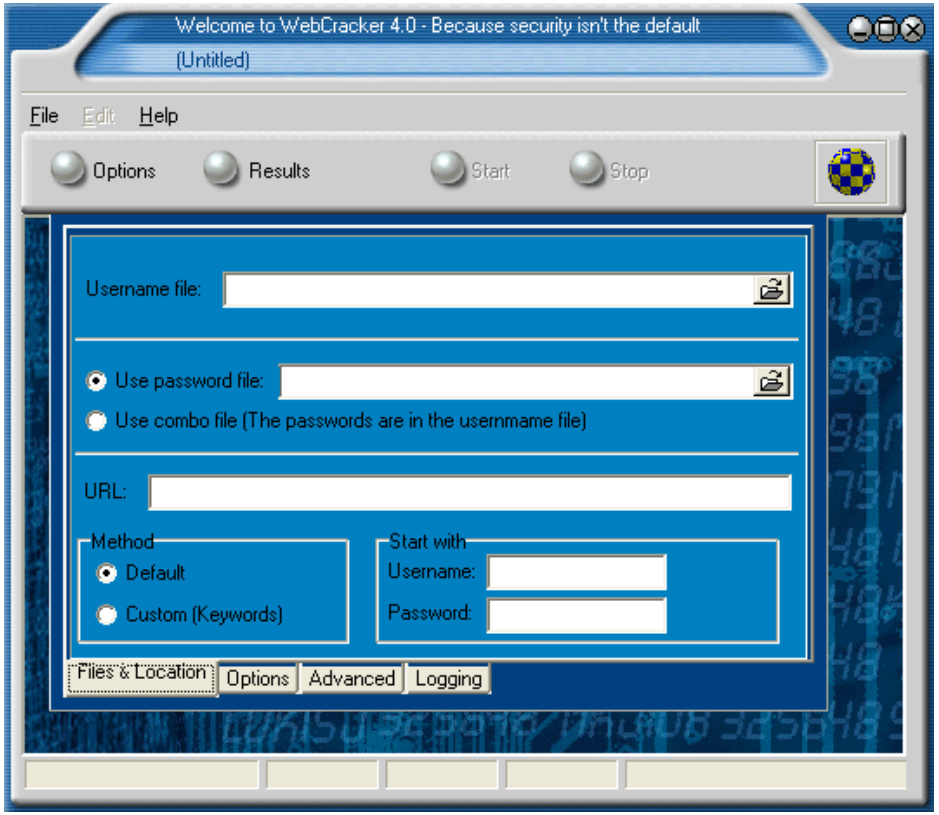
- Brutus

- Brutus AET2 是一個破解工具，可以破解以下驗證類型：HTTP、POP3、FTP、SMB 遠端登入、NNTP、NetBus...等，還可以自行設置字典檔。



工具程式

- WebCracker
- WebCracker是破解密碼的軟體，主要對需要密碼的網站進行暴力法破解 。



工具程式

- John The Ripper
- 一個彈性的、快速的、多平台的密碼破解器。
- 主要的功能是能夠偵測弱密碼，它支援幾種加密的密碼形態、Kerberos AFS、Windows NT/2000/XP LM hashes…等。

WinSSLMiM

- WinSSLMiM是HTTPS man-in-the-middle的攻擊工具，它包含了一個工具FakeCert用來產生仿造的查驗。