

Dopo la guida „Come fare PUB Scans” passiamo alla seconda Lezione:

Come fermare i Deleters

Chi sono i Deleters?

In genere è gente come noi, che però dopo aver scaricato i files cancellano tutto! Un altro motivo che spinge questi stronzi a cancellare gli uploads degli altri per esempio può essere mancanza di space o banda su un pub che usano anche loro stessi.

Noi non vogliamo mica vedere tutti i nostri sforzi buttati nel cesso vero?

Questa guida ha lo scopo di insegnare a tutti come proteggere i loro pub dai delters, o almeno da quelli non super-esperti!

Chi è il SysAdmin (System Administrator)?

È colui che lavora per l'azienda che è in possesso del pub che noi gli abbiamo fottuto! Questo appena sente puzza di bruciato (Connessione troppo lenta, troppa banda consumata o HD pieno!!) chiude il server o toglie l'accesso anonimo! E questo non si può fermare. ☹

Ok iniziamo...

Per prima dobbiamo proteggere le cartelle stesse!

Come fare cartelle inaccessibili?

C'è da dire che le tecniche con server NT e UNIX non sono le stesse, ma molto diverse! Se non sapete che OS c'è sul pub pescato, basta guardare mentre vi loggate.

- **Server NT**

Nel root del server bisogna cercarsi un posticino non sospetto al SysAdmin, per esempio:

```
/~/  
/images/  
/_vti_pvt/  
/_vti_cnf/  
/_vti_log/  
/temp/  
/tmp/
```

// <- Questa cartella è invisibile, quindi non si vede con un FTP Client, se poi il SysAdmin la vede non lo so.

Ovviamente bisogna anche guardare dai risultati dello scan in che cartelle avete i permessi!

Dopo aver creato una prima cartella **bisogna** inserire una cartella inaccessibile!

Le cartelle inaccessibili sotto NT sono:

COM1 COM1 COM3 COM4 (Windows COM PORTS)

LPT1 LPT2 LPT3 LPT4 (Windows Printer Ports)

AUX

NUL

Scelta quella che vi piace di + (la funzione è la stessa per tutte!) bisogna fare così per poterla inserire:

Per prima cosa create una cartella

COM1//

ripeto

COM1/<1spazio>/

Poi rifare la stessa directory ma così:

COM1/PAROLA CHIAVE/

Per poter superare la cartella COM1 (o quello che avrete scelto dalla lista di sopra) bisogna per forza sapere la prossima cartella, in questo caso PAROLA CHIAVE. Dato che è la chiave per entrare non consiglio di usare parole troppo comuni tipo Tagged o Scanned, perché sono le prime cose che un deleter prova.

Esempio:

/_vti_pvt/**COM1/leon**/Scanned by/SCANNER/4/BOARD/Filled by/UPLOADER

Cartella protetta, Parola chiave

In questo modo per entrare dovrai bisogna tutta la path intera quindi COM1/leon/

Chiaro no? Ok allora andiamo avanti!

- **Server Unix (BSD, SunOS etc)**

Con questi server i trucchetti COM1 etc non funzionano dato che quelli sono comandi Windows! Ma anche qui ci sono i trucchetti da usare! Qui la storia si fa un po' + complicata, ma non troppo! C'è anche da dire che su server Unix gli accessi si hanno quasi sempre nella cartella /incoming/.

Cercatevi un posicino al calduccio e dopo inserite la cartella protetta... si fa così:

(quanti spazi volete).NOMECARTELLA;;(quanti spazi volete)

Esempio:

(6spazi).sparisci;;(10spazi)

Avvertimento: Per poter passare questa cartella bisogna sapere (non la prossima cartella come con NT) i spaces che avete usato! Se dimenticate i spaces non entrate +!

Se volete, prima di questa cartella inaccessibile si può inserire (non va sempre però) anche una cartella invisibile, basta fare una cartella così:

(spazio)../

Tutto chiaro no?

Esempio:

/../ .sparisci;; / Scanned by/SCANNER/4/BOARD/Filled by/UPLOADER

Cartella invisibile, Cartella inaccessibile

Adesso passiamo alla seconda fase:

Come rendere i files incancellabili?

Questa tecnica è molto facile, ma un pochino faticosa se si hanno tanti files... mo vi spiego.

Allora bisogna rinominare **ogni** file uppato così:

file.zip (originale)

file.zip ./ / (truccato)

ripeto: file.zip<1spazio><punto>/<1spazio>/

In questo modo i file non saranno più cancellabili, neanche da chi li ha uppati!

Molto spesso con i server UNIX questa tecnica non funziona.... Se il server è NONDELTABLE ovviamente non c'è bisogno di rinominare tutti i files, anche perché non va! ;)

Siamo arrivati alla fine, spero di esservi potuto essere di aiuto anche con questa guida!

Alla prossima guida allora! ;)

G|G3TtO

Un ringraziamento a Morpheus che all'epoca mi passò tutti i doc trovati in giro! Thx Morph!