

Come fare PUB Scans

OK, questo è un Tutorial Step-by-Step fatto per quelli che non hanno nessuna conoscenza in materia, quindi non andrò molto nel dettaglio! Lo scopo è quello di poter far imparare ad altri l'arte del fare pub.

Un Pub è un server FTP con accesso anonimo e che permette sia la lettura che scrittura! Quindi permette anche di poter creare cartelle e poterci uppare dentro. Uno svantaggio è che si può anche cancellare il contenuto (FuCk Ya DeLeTeRz!)? Il nome Pub risale dalla cartella "pub" presente su molti server FTP (dove spesso volte si ha anche il diritto di scrittura) o anche dal nome stesso "Public FTP".

Ok, adesso dopo aver spiegato un pò di teoria, passiamo alla pratica! Ma a che cosa servono questi pub poi? Molto semplice, per poterci uppare sopra dei files. Poi questi pub "offrono" molto + spazio che i semplici servizi gratuiti di Webspaces! In molti casi questi server sono anche molto + veloci! Cmq dipende. Si distinguono tra "Win NT" (Versione 4 o 5), "Unix" (FreeBSD o altro!) e molto raramente anche "SunOS"! Ecco, sono questi i Sistemi Operativi che usa la maggior parte dei server FTP! Quelli con WinNT sono i + comuni, maggiormente versione 4! Questa versione contrariamente alla 5 non supporta il RESUME!
+ rari, ma anche + importanti sono i server Unix! Anche qui ci sono quelli con Resume e quelli senza! Cmq sono molto importanti per Fxpare (ne parleremo in un secondo manuale)!

PUH! Adesso facciamo sul serio!!! ;)

Cosa ci serve?

1. Grim's Ping (ultima versione, scaricabile qui: <http://grimsping.cjb.net/>)
2. Moltissima pazienza!
3. Un pò di esperienza con i server FTP è di vantaggio, ma non deve essere...

Ecco! Tutto qua!!! ;)

Adesso partiamo! Per prima cosa scaricatevi l'ultima versione di Grim's Ping, e poi una volta installato andate in File -> Options (oppure semplicemente F8) -> Permissions e attivate "Log Directory Permissions", poi andate in "Logging" e attivate tutto a parte "Exclude nondeletable pubs from log". Siete pronti per fare i vostri primi scans!

Io nel frattempo vado a fare colazione... e poi torno! ;)

Ok, finito, adesso si continua...

Adesso viene uno dei + difficili, ma anche + importanti passi: La scelta degli IP-Ranges, cioè gli IP su cui si vuole fare lo scan!!! Ci sono vari modi, questa è sicuramente la + facile e + semplice per i novellini.

Per prima cosa bisogna andare su un motore di ricerca, come per esempio Altavista o Google, e cercare delle parole chiavi, che siamo sicuri che porteranno molti risultati, per esempio Software, Download, Internet, XXX o che so io! Prendete uno di questi link a caso e copiate il

collegamento! Adesso aprite Grim's Ping e premete F9 (single host lookup)! Facendo Host Lockup scoprirete l'IP del server (quello che vogliamo no?). Dunque inserite il link copiato in precedenza togliendo i vari "/" e "http". È importante questa procedura.. per vedere se avete capito vi faccio un'esempio!

<http://www.abcdefgh.com/abcdef/index.html>

Dovete eliminare tutto, in modo da far rimanere solo il dominio stesso

www.abcdefgh.com

Chiaro no? :-)

Un consiglio: Prendete solo link .com/.co.uk/.de/.ch/.it etc! In nessun caso .mil/.edu/.gov etc, perché poi diventa pericoloso, a meno che non si usi un sock, ma questa è un'altra storia.

Adesso avete ricevuto un IP tramite Grim's Ping! Questo lo dovete copiare e poi andare su Tools -> Add query entry (o semplicemente F6) e andare su "Paste" e inserire l'IP. Cosa succede adesso? Mettiamo che l'IP fosse 154.62.216.64, quindi adesso verrebbe fatto lo scan di ogni IP da 154.62.216.1 a 154.62.216.254, tutto il Range praticamente!

Ma questo non è sufficiente per noi! Rincominciate tutto e aggiungete altri Ranges in coda così da poterci anche allontanare dal PC! Ogni volta in questo ordine: cercare, scoprire l'ip, inserire l'ip e tutto da capo....

Adesso nella schermata principale di Grim's Ping dovrete avere in basso vari Ranges in coda! Non dovete fare altro che premere sul semaforo per partire!

Mentre lo scan procede, è possibile visualizzare lo Status nella schermata principale. Qui si può notare Request Timed Out (l'IP no esiste!), Connection Forcefully Rejected (Errore del server), User Unknown (il server non permette l'accesso anonimo!) oppure LOGIN CORRECT!! :-)))))) Premendo F3 verranno visualizzate tutti i server (IP) che hanno l'accesso anonimo.

Adesso avete un server che permette l'accesso ANONIMO! Ma questo ovviamente non basta! Volete avere anche il diritto di scrittura no?!

Quindi anche se avete trovato 100 volte Login Correct, non vuol dire che avete 100 Server utilizzabili! A volte nemmeno uno! "Addirittura!!!" starete pensando, ma ecco quello che dicevo all'inizio, uno dei requisiti è la PAZIENZA, quindi non vi dovete abbattere, prima o poi si trovano anche i pub buoni!

Continuiamo? ;-)

Premendo F2 invece, verrà visualizzato il file perm.log, questo è il file dove verranno salvati tutti i server (IP) che permettono non solo l'accesso, non solo la lettura, ma anche la SCRITTURA, ed è questo che vogliamo!!

Non smettete, anche se per molto tempo forse rimarrà vuoto il file, continuate a fare lo scan. Il pensiero di poter presto trovare un pub non vi stuzzica?

Ok, adesso dopo molti (o forse pochi... chi lo sa) tentativi avete finalmente trovato il vostro pub. Sempre nel perm.log (F2) verrà visualizzato se il server supporta FXP (importante!) in quale cartella avete il diritto di SCRITTURA, se è cancellabile e quale Sistema Operativo usa! Continuate fino a che non troverete dei buoni server e magari anche sotto UNIX!

Ancora una volta: Potete usare SOLO i pub presenti nel perm.log (F2), su gli altri non avrete il diritto SCRITTURA, non utilizzabili quindi!

Ci siete riusciti, adesso anche voi siete in grado di cercare dei pub VOSTRI!

Vi auguro molto divertimento nei vostri futuri scans! ;)

G|G3TtO