Autor: Yoyahack
Fecha: 5/9/2009
Web: yoyahack.blogspot.com
Mail: yoyahack@hotmail.com
Webs: www.undersecurity & www.mitm.cl

En que consiste esta técnica Reverse DNS ¿?

Bueno algunas veses queremos prenetar un servidor web pero no encontramos una vurnerabilidad, o si no es otra cosa, o si es una web que esta hecha al 100% html su put... Pues no podemos ingresar y poder darle bueno lo que podemos haser es haserle un Reverse DNS, osea ver si la web esta compartida, podemos haserle un scan pueden ir a esta web:

http://www.myipneighbors.com

Ok escriben la web que quieren atakar y si la pagina esta compartida podemos usar otra web para poder atakar nuestro objetivo principal, loque hase la pagina es buscar todo los dominios con la misma ip de nuestro objetivo, si saca una pagina esque esta compartida imaginen, un ejemplo

Web por atakar:

www.atakar.com

Web con la que podremos usar para atakar atravez de ella:

www.pagina.com

oka loque podemos haser es encontrar una vurnerabilidad wn www.pagina.com y atravez de hay atakar a www.atakar.com , bueno loque debemos haser es buscar una vurnerabilidad en www.pagina.com y tratar de subir una backdoor o si no una phpshell para mas comodida, listo ahora cuando subimos la phpshell imaginence que el path de www.pagina.com es el siguiente:

/www/sites/pagina.com/

lo que hasemos es lo siguiente:

/www/sites/atakar.com/

y ingresamos a esa otra web y se preguntaran pero como puede suceder eso, bueno aqui le explico unas cositas:

si la ip de www.atakar.com es: 168.69.58.1
y la de www.pagina.com es: 168.69.58.1
Son la misma lo que significa que estan en el mismo Servidor, porque enrealidad un hosting es un ordenador y los dominios son carpetas y en las
carpeta /www/sites/ estan todos los dominios compartido podemos atakar a todos mediante uno en eso consiste este atake.

Otra cosa que hay que tener encuenta que algunas veses no podemos ir a las otras web porque no tenemos permiso, en ese caso debemos rootearlo jejej, saludos.