Shell доступ за 10 минут

[Хакерство в Интернете]

Надеюсь, что такое шелл - вам объяснять не надо. Ребята с бронепоезда могут пропустить данную статью, а тем кто все еще со мной, я хочу рассказать об одном эффективном методе получения тех самых шелов. Как то раз, один мой знакомый посоветовал мне пойти в поисковую систему и поискать файлы типа: .htaccess, order.html, .bash_history, etc … К моему удивлению, поисковик выплюнул несколько .htaccess файлов и что то еще, сейчас точно не помню. Но прошли те времена, когда такое было возможно, хотя если хорошо поискать, возможно, и найдете чего. Не буду вспоминать о прошлом, а перейду непосредственно к нашей сегодняшней теме. Как я упомянул чуть раньше, поисковая система может искать не только рефераты и порнуху :). Попробуем поискать скрипт из популярной доски объявлений ikonboard - help.cgi, в котором недавно была найдена уязвимость, которая позволяет просматривать любые файлы в системе с правами вэб сервера. В результате вы получите листинг сайтов содержащих данный скрипт. Кстати говоря нередко можно наткнуться на такую ситуацию, что у скриптов могут быть изменены расширения с .cgi на .pl и наоборот. Либо весь пакет может быть установлен в /cgi/ - поэкспериментируйте с поисковыми значениями. После того как нашли интересующий скрипт, следующим шагом будет хорошо знакомый 'cat etcpasswd'. Здесь может быт несколько вариантов: вы получаете passwd файл с паролями в DES (что маловероятно); затененный passwd файл (70 %); сообщение о том что ваш IP записан в лог + обзовут нехорошим словом :); скрипт пропатчен либо файл не найден. С DES я думаю ты и сам разберешься, а вот затененный passwd это гвоздь программы на сегодня. Многие забывают о сайте не получив желаемого passwd с DES хешем, а вот зря! Сейчас объясню почему. Вы никогда не задумывались о том, что компьютеры становятся быстрее и мощнее, операционные системы гибче и надежнее, а люди в своем большинстве остаются теме же. Да да, я говорю о паролях, которые до сих пор остаются довольно простыми и чего хуже, совпадают с именами пользователей. На этом мы и сыграем. Получив passwd, скачаем программку "passwd splitter" из раздела "projects" на нашем сайте. После этого обработав ею наш passwd - получим файл с одними именами пользователей. Далее скормим этот файл SSS (shadow security scanner в режиме user=password - в принципе можно воспользоваться любой brute force программой) с проверки паролей на FTP доступ. FTP выбран потому что через него производиться наиболее быстрый перебор паролей. В 70% случаев пользователи имеющие FTP доступ - имеют telnet доступ. Если нет ftp можно перебирать через telnet, но это намного медленнее. После перебора, нередко можно удивиться доступу в систему через telnet. Это не выдумки, а действительность, которой подвержено достаточно большое количество систем, где обязательно найдется человек с "хорошей памятью", у которого имя пользователя совпадает с паролем. А как понимаете имя локальный доступ, root shell уже не далеко. Данный метод довольно примитивен, но зарекомендовал себя неплохо. Так что не забывайте посещать сайты охватывающие проблемы компьютерной безопасности, на которых публикуются последние уязвимости в cgi скриптах. Безусловно, то, что я описал в этой статье пригодиться в любой ситуации, где у вас есть доступ на чтение passwd файла, например в институте где у студентов есть шел доступ к unix системе, но в России вариант user=password навряд ли прокатит ;).