Взлом HTTP паролей с помощью программы Xavior

Ну что же здарова кул-хакЁр!!!Ты ещё не кул-хакер???Ты ещё не натянул сервак www.whitehouse.gov??? Ты ещё даже не научился выкидывать ЛОМОВ из чата??? Ну так что же, не беда, этому ты научишься позже...

Вот задаёшься ты вопросом: как же этот кул-хакер взломал твоё вэб мыло и от твоего имени рассылает коников и вирей??? Ну ничего сегодня мы тебе расскажем как это делается самым простым способом. Для этого тебе не понадобятся какие-нибудь углубленные знания генной инженерии и знания азбуки Морзе, а так же не понадобится понятие принципа работы электронного розгонятиля протонов в вакууме.

Ну так вот, сначала валишь на http://guest.btinternet.com/~lithiumsoft/xavior/Download.html и сливаем себе рулезную прогу под названием Xavior v1.0 Beta 7.Инсталим,там ничего сложного и сверхъестественного, вот у нас уже есть оружие начинающего Хакера.

Вот запустил ты енту прогу на своей тачке и видишь уродство и говоришь себе: "Блин что это за убожество, отстой, ни картинок тебе, ни нормального ХЕЛПА..." (у меня так и было...=)Но всё пока ты не понимаешь ценности этой вещи. Ну вот например я тебе напишу неполный список того что ты можешь сделать с помощью этой проги:

подобрать пароль к мылу своего заклятого врага и поотсылать от его мыла выря или лошадку(ну тока не Прижевальского, ну да ты сам знаешь...)

поломать ТЕХ. ПОДДЕРЖКУ своего ПРОВА и раздобыть себе ХАЛЯВНЫЙ АККАУНТИК и делать далее усё что твоей хацкерской душеньке угодно (даже продать его=)

раздобыть себе АККАУНТИК к ПОРНУШКЕ и даже если ты таким не увлекаешься (может ты этакий КАЗАНОВА и на этих баб, тем более в голом виде уже смотреть не можешь, тошнит=), то есть много людей готовых за такой АККАУНТИК сделать ТтАаКкОоЕе!!!...уже проверенно...=)))

Ну и многое другое, надеюсь ты сам понимаешь...

Ну хорошо приступим к описанию самой проги. Вот запустил ты её и смотришь...а что же тут делать, а вот сейчас я это и объясню...

Перед тобой менюшка с 6 закладками, о каждой по порядку:

1)Information-это закладка в которой есть такие опции как:

Usernames File-енто файл в котором задаются ЛОГИНЫ

Passes File-это файло в котром задаются ПАРОЛИ

Currently Position Filename-это файл с расширением \*.xvp. Вот это и есть хорошая фишка этой програмульки, это значит что ты можешь долбать спокойно какой-то мыл и в нём сложный пасс и требует долгого и упорного долбления, а тут как раз время ночной халявы кончается =).И что делать ты думаешь, а ничего не надо, будет всё снова начинать!!! Прога запомнит позицию долбления и потом начнёт с неё.

Далее идёт status, то есть online или offline (где-то я уже это видел, вот тока никак не припомню=).В правом углу идёт усякая ИНФА типа номера сессии, попыток в секунду, оставшееся время и т.п. Внизу есть 2 окна: первое-всякая инфа ненужная, позиция долбинга (во как сказанул=),второе-окно это списки ЛОГИНОВ и ПАССОВ которые прошли или заканали...кто как называет.

2)закладка General Options-это собственно говоря усе опции, а то есть:

Target(Adress/IP) - ну это адресок того, что собираемся долбить. Port-это порт по которому долбится будем, по умолчанию 80(HTTP)

Directory/File (For WEB servers) - ну а это папка на серваке куда долбится будем, по умолчанию /secure

-Program to masqurade as...-это под что прога шифруется

Number оf Sesions-это кол-во сессий

Далее надо поставить галочку на Auto Save Position every 100 attemps. Потом идёт выбор куда же именно на серваке долбится будем, то есть:

Standart HTTP basic Authentication - это стандартная проверка ЛОГИН\ПАССА

CGI-BIN/POST - это определение ПАССА\ЛОГИНА по CGI и в ФОРМАХ

Scripting-это по скрипту

И вот последнее в этой закладке:

Checking Method-метод проверки=):

Loop throught passwrds file once for every user-это прыгать по ПАССАМ на 1 ЛОГИН,потом на 2 ЛОГИН и опять прыжки по ПАССАМ

Make passwrd equal to username-это как я понимаю прога берёт 1 пасс и прыгает по ЛОГИНАМ,вроде так

Brute Force all character combinations-вот это самая рульная вещь,тобиш БРУТ ФОРС или подбор по буквам

3) 3акладка Scripting-установки скрипта.

4) 3акладка Mutators-это мутаторы с помощью их можно например сказать проге что-бы юзала ПАССЫ и ЛОГИНЫ только в маленьких буквах.

5) 3акладка Brute Forcing-установки БРУТ ФОРСА или наборы символов.

6) 3акладка Advanced - вот нужная в натуре вещь, поподробней:

Use WWW Proxy-Web PROXY adress-Port - ну енто использование ПРОКСИ сервака, вещь архинужная и архиважная! Но вот пока не могу понять почему же по умолчанию она отключена %-Е

Sleep between multiple sessions... - пока сам понять не могу нафига оно надо...?

Minimize To Tray - без комментариев...

Use timeouts - это время отдыха проги между долбингом,советую отключить вообще

Log Accepted Names/Passes to "accepted.log"-енто записывать удачные ЛОГИНЫ и ПАССЫ в этот файл.

Ну да ладно этой усей инфы,я лучше расскажу всё на примере: вот например есть ПРОВ и я знаю ЛОГИН (если у юзверя есть мыло, то адрес до @ и есть как всегда ЛОГИНОМ) и знаю что пасс у него состоит где-то из 6 знаков. Мутим раз - берём Melco$oft Notepad-и пишем там ЛОГИН, например superlamer, то бишь мыло у него будет примерно такое: superlames@megaprov.com. Дальше берём любой генератор паролей и задаём ему сгенерировать 1000 паролей с большими и маленькими буквами и с цифрами...есть??? Молодец!!!

Мутим два - осталось настроить прогу и в путь!!! Значит ставим в проге тот именно файл с ЛОГИНОМ который мы там писали (superlamer),подставляем файл с ПАССАМИ которые нам добротно сгенерировала прога-генератор паролей. Дальше ставим адрес, например www.users.superprov.com, отключаем таймаут, включаем прокси (даже если у тебя уже стоит ПРОКСИ, всё равно включи как говорится "Оперативкой КОМП не испортишь!"=), ставим галочку на log accepted...указываем файло для сохранения попыток, что-бы не начинать при обрыве связи всё с начала, и совсем забыл (БООТ сектор у меня дырявый видно=) поставим ГАЛКУ в закладке General Options на Auto Save Posichion every 100 attempts!!!

Всё, ты готов к ворованию аккаунта. Идём в меню Actions (это там вверху) и жмём GO!!!

В заключении хочу сказать что если усё сделано правильно, то должно получится... но надо помнить что разные серваки построены на разный ОС и это может и не заканать. И ещё надо всегда помнить что: ЖАДНОСТЬ ХАКЕРА СГУБИЛА!!! Так что вперёд к новым барьерам (аккаунтам, мылам и т.п.)

Удачного тебе ХАКА мой маленький электронный вор!!!=)