

УДК 004.728.4.056.53

ПЕРЕХВАТ ПАРОЛЕЙ В ОТКРЫТЫХ WI-FI СЕТЯХ С ПОМОЩЬЮ ПРОГРАММЫ INTERCEPTER-NG

Ерошевич К. В, студент гр. ИТб-132, 4 курс
Научный руководитель: Алексеева Г.А., ст. преподаватель
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

В наше время широко распространены открытые точки доступа Wi-Fi. Но мало кто задумывается о сохранности своих персональных данных подключаясь к открытой точке Wi-Fi.

Подключившись к открытой точке Wi-Fi, можно обеспечить доступ к своим персональным данным третьим лицам, не поняв этого.

В качестве примера будет рассмотрена программа Interceptor-NG. Данная программа позволяет не только перехватывать пароли от сайтов, но и заменять сайты и многое другое.

После запуска программы, нужно выбрать сеть в графе «Network Adapter», к которой подключен компьютер (рисунок 1).

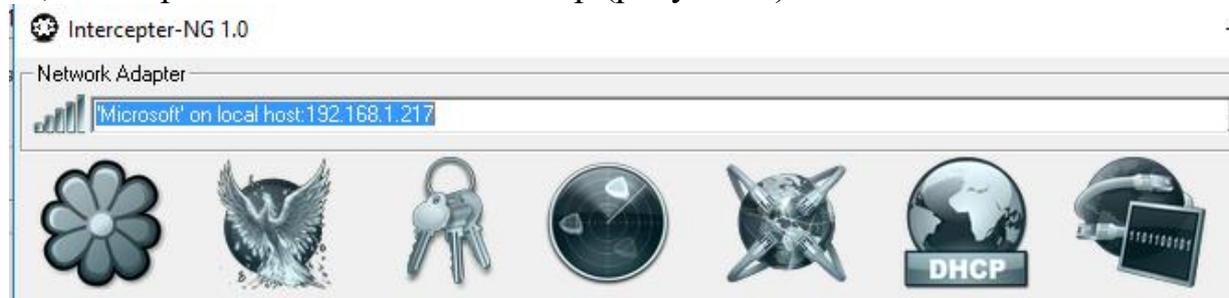


Рисунок 1

Следующим шагом производим настройку программы. Окно настройки представлено на рисунке 2.

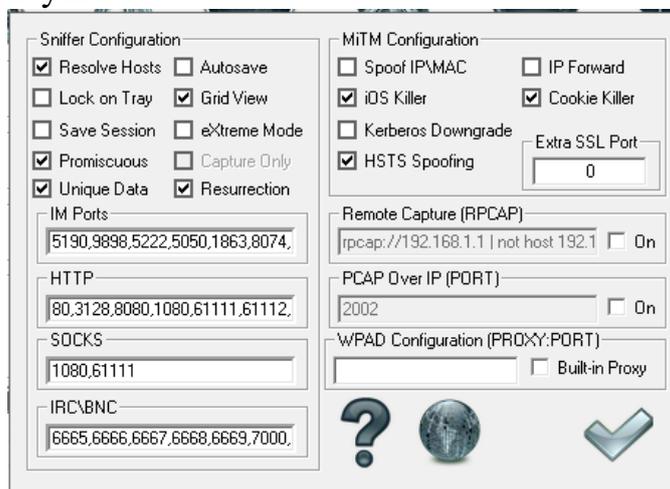


Рисунок 2

Следует отметить следующие опции:

- Resurrection для перехвата Cookie HTTPS;
- Cookie Killer, чтобы заставить пользователя снова вводить пароль.

После проведенных манипуляций необходимо запустить программу.

Далее нужно выбрать в меню пункт «MiTM Mode» и в «MiTM Option» следует нажать на изображение, отмеченное на рисунке 3 цифрой 2.

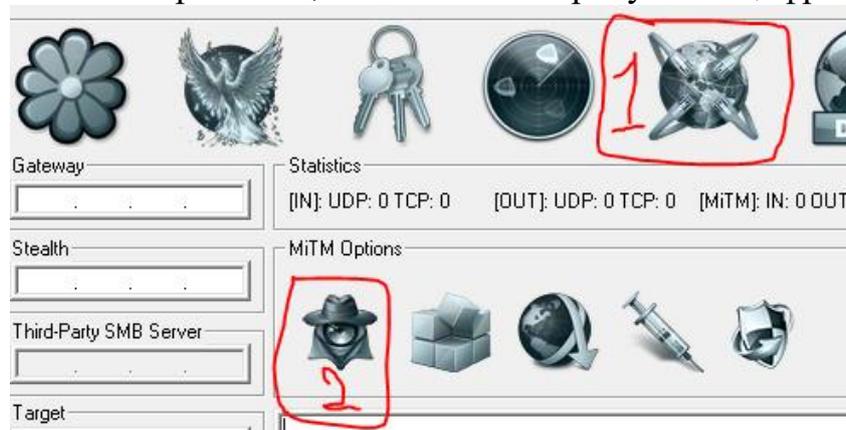


Рисунок 3

В открывшемся окне (рисунок 4) нужно отметить «SSL MiTM» и «SSL Strip».



Рисунок 4

Выполним еще пару действий и программой можно пользоваться. Перейдем в соответствующую вкладку и выберем пункт «Smart Scan». Появятся все устройства, подключенные к сети Wi-Fi. Выбираем объект и в контекстном меню пункт «Add as Target» (рисунок 5).

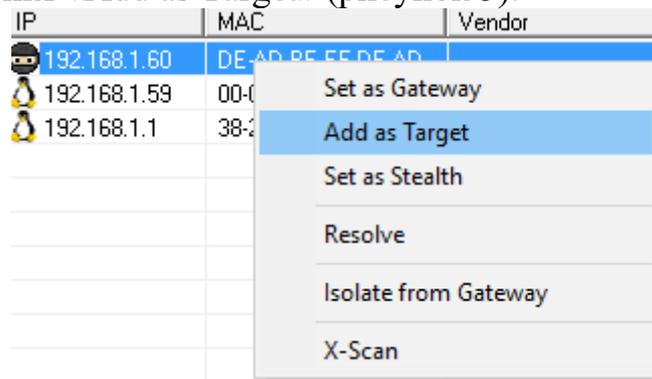


Рисунок 5

Далее перейти на вкладку с изображением ключей. В этой вкладке будут отображаться логины и пароли, введенные объектом перехвата на сайтах.

В качестве примера рассмотрим на сколько защищены сайты aist.kuzstu.ru (HTTP протокол), portal.kuzstu.ru (HTTPS протокол).

1. Сектор содействия трудоустройству выпускников aist.kuzstu.ru

Введенные данные логин: User; пароль: password (рисунок 6).

Рисунок 6

Результат работы программы представлен на рисунке 7.

Protocol	Time/Date	From/To	Host	Username	Password
HTTP Auth	21:34:54...	192.168.1.59/193...	aist.kuzstu.ru/index....	username=User	&password=password

Рисунок 7

2. Портал КузГТУ portal.kuzstu.ru

Введенные данные логин: User; пароль: password (рисунок 8).

Рисунок 8

Результат работы программы представлен на рисунке 8.

Protocol	Time/Date	From/To	Host	Username	Password
HTTP Auth	21:34:54...	192.168.1.59/193...	aist.kuzstu.ru/index...	username=User	&password=password
Web Site visited	21:38:32...	192.168.1.217/19...	192.168.1.217	portal.kuzstu.ru	
HTTPS Auth	21:38:51...	192.168.1.217/19...	portal.kuzstu.ru/auth...	username=User	&password=password

Рисунок 8

Как видно программа работает даже в случае использования HTTPS протокола.

Из всего выше сказанного можно сделать следующий вывод перехватить персональные данных легко, а «подарить» их еще легче, даже если Вы пользуетесь сайтами по HTTPS протоколу. Поэтому прежде чем воспользоваться открытыми Wi-Fi точками доступа, следует очень хорошо подумать, так как неизвестно кто и для каких целей может ими пользоваться вместе с Вами.

Список литературы:

1. Interceptor-ng.com[Электронный ресурс] URL: <https://interceptor-ng.com>