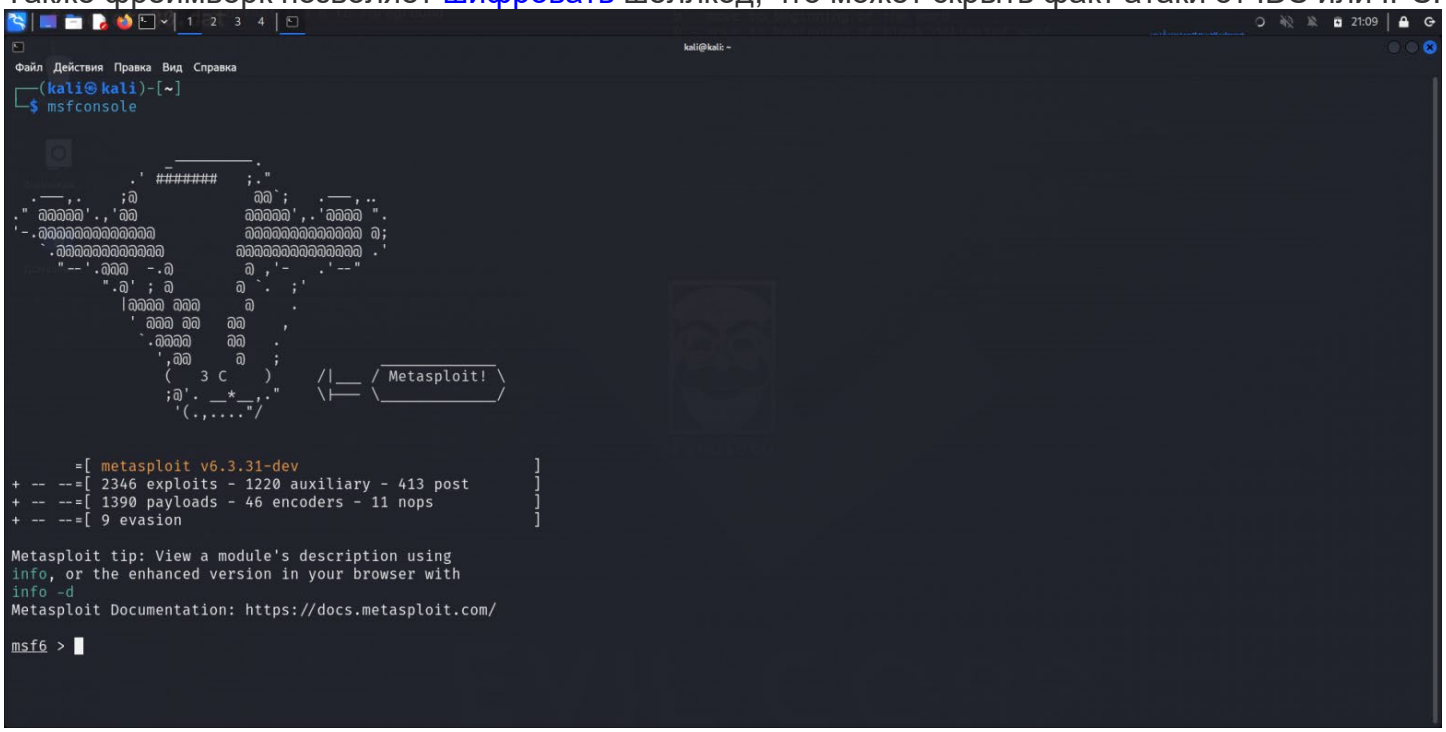
Популярные инструменты в Kali Linux

Metasploit framework

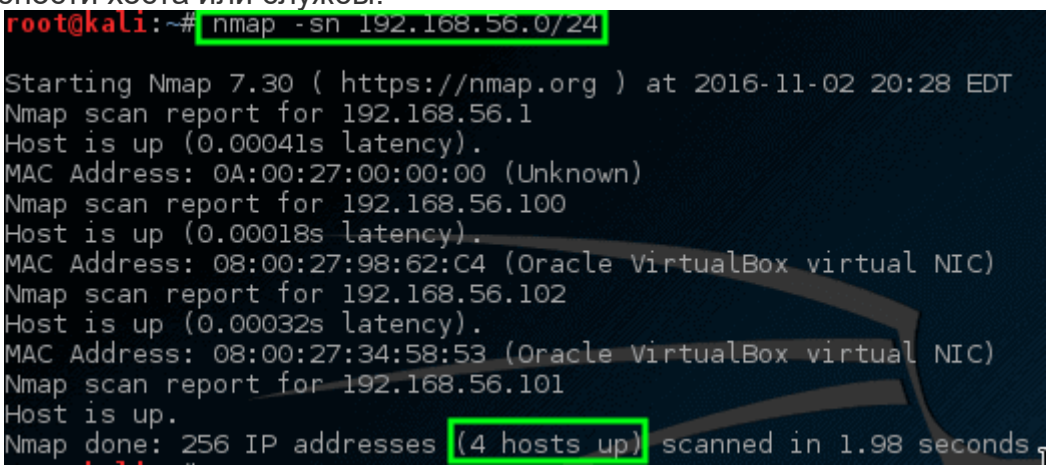
Инструмент для создания, тестирования и использования эксплойтов. Позволяет конструировать эксплойты с необходимой в конкретном случае «полезной нагрузкой» (payloads), которая выполняется в случае удачной атаки, например, установка shell или VNC сервера. Также фреймворк позволяет шифровать шеллкод, что может скрыть факт атаки от IDS или IPS.



metasploit

Nmap (Network Mapper)

Это свободная утилита, предназначенная для настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб). Nmap обычно используется для аудита безопасности, многие системные и сетевые администраторы находят это полезным для повседневной работы такие задачи, как инвентаризация сети, управление обновлением услуг расписания и мониторинг работоспособности хоста или службы.



nma

Wifite

Это автоматизированный инструмент для атак на беспроводную сеть. Работает с привязкой wifi адаптер. Не все поддерживает адаптеры к kali, нужно выбрать с умом. Вот самые популярные адаптеры:

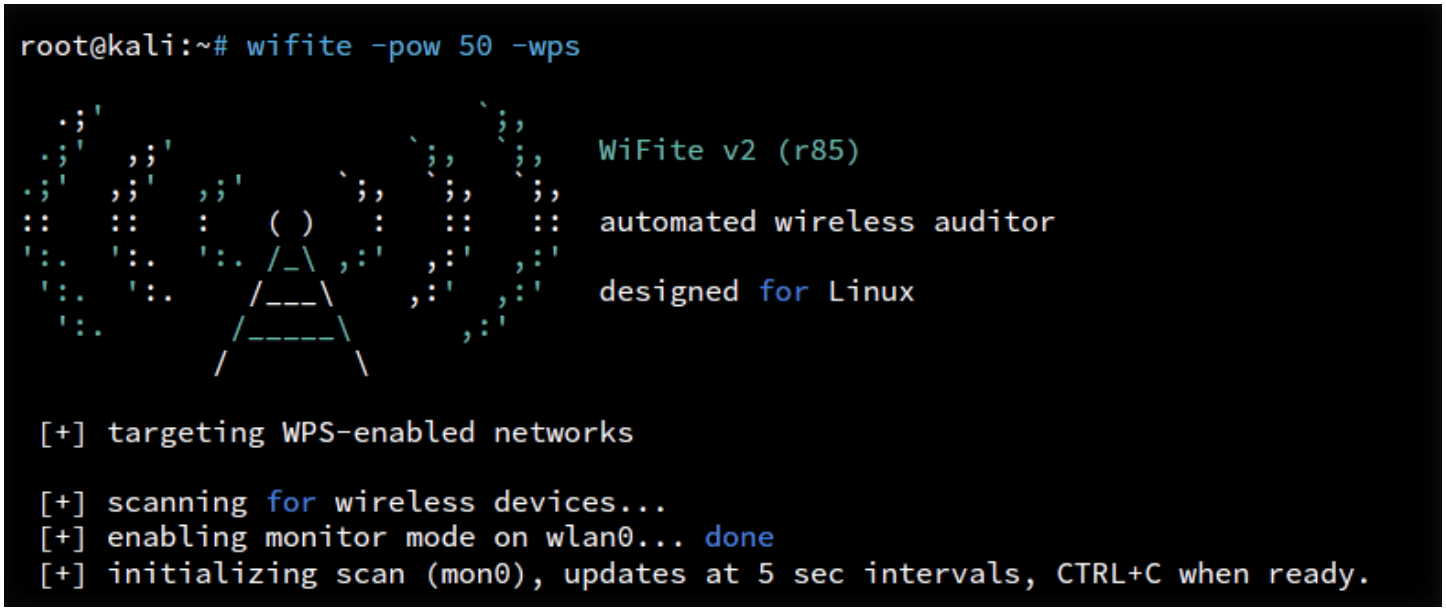
Alfa AWUS036NHA

Alfa AWUS036ACH

Alfa AWUS1900 / AC1900

Panda Wireless PAU09

Panda Wireless PAU06



Sqlmap

Sqlmap - это инструмент тестирования на проникновение с открытым исходным кодом, который автоматизирует процесс обнаружения и использования ошибок SQL-инъекций и захвата серверов баз данных. Он поставляется с мощным механизмом обнаружения, множеством специализированных функций для идеального тестера на проникновение и широким набором переключателей, начиная от снятия отпечатков пальцев с базой данных, выборки данных из базы данных и заканчивая доступом к базовой файловой системе и выполнению команд в операционной системе через внешний интерфейс. внеполосные соединения.

John The Ripper

John The Ripper - это инструмент с открытым исходным кодом для взлома паролей методом перебора. Изначально он был разработан для Unix, но сейчас доступен на всех Unix-подобных платформах, в том числе и Linux. Программа также известна как JTR или John. Она наиболее часто используется для перебора паролей по словарю.

Программа берет текстовую строку из файла, шифрует его таким же образом, как был зашифрован пароль, а затем сравнивает зашифрованный пароль и полученную строку. Если строки совпадают, вы получаете пароль, если нет, программа берет другую строку из текстового файла (словаря). Именно с помощью этого инструмента можно проверить насколько надежны пароли в вашей системе.

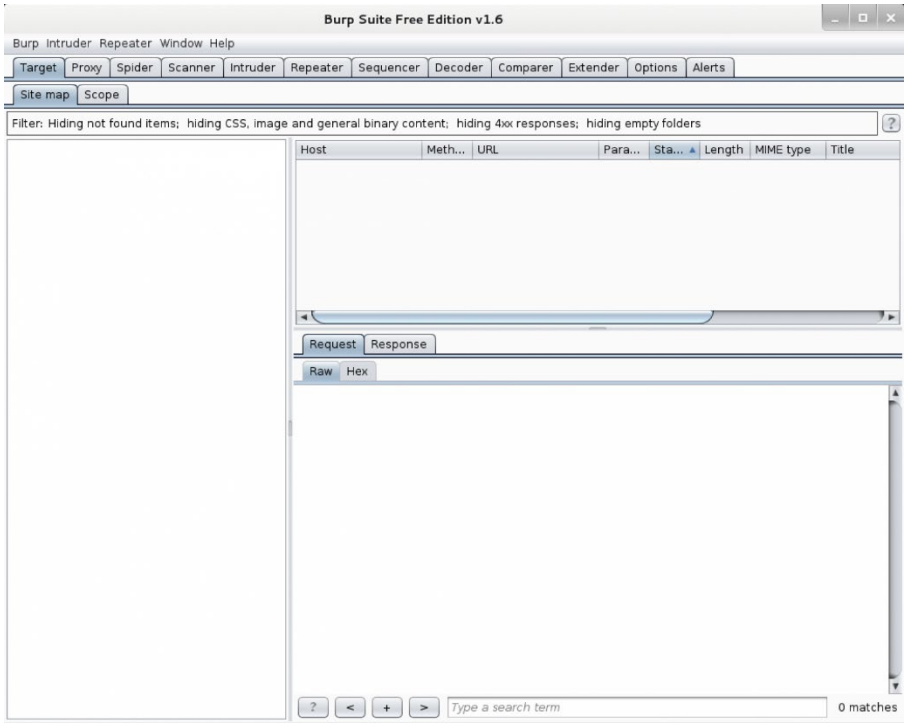
```
root@kali:~# unique
Usage: unique [-v] [-inp=fname] [-cut=len] [-mem=num] OUTPUT-FILE [-ex_file=FNAME

       reads from stdin 'normally', but can be overridden by optional -inp=
       If -ex_file=XX is used, then data from file XX is also used to
       unique the data, but nothing is ever written to XX. Thus, any data in
       XX, will NOT output into OUTPUT-FILE (for making iterative dictionaries)
       -ex_file_only=XX assumes the file is 'unique', and only checks against XX
       -cut=len  Will trim each input lines to 'len' bytes long, prior to running
       the unique algorithm. The 'trimming' is done on any -ex_file[_only] file
       -mem=num.  A number that overrides the UNIQUE_HASH_LOG value from within
       params.h.  The default is 21.  This can be raised, up to 25 (memory usage
       doubles each number).  If you go TOO large, unique will swap and thrash an
       work VERY slow

       -v is for 'verbose' mode, outputs line counts during the run
```

Burp Suite

Burp Suite - это инструмент для поиска уязвимостей на сайтах интернета и в веб-приложениях, который может работать как по HTTP, так и по HTTPS. Он используется многими специалистами для поиска ошибок и тестирования веб-приложений на проникновение. Программа позволяет объединить ручные методы со своими средствами автоматизации, чтобы выполнить тестирование как можно эффективнее. Burp Suite написана на Java и распространяется в формате Jar.



Nikto

Nikto - это подключаемый веб-сервер и сканер CGI, написанный на Perl с использованием LibWhisker RFP для выполнения быстрых проверок безопасности или информации.

Функции:

- Легко обновляемая база данных чеков в формате CSV.
- Вывод отчетов в виде обычного текста или HTML
- Доступные версии HTTP с автоматическим переключением
- Общие и специальные проверки серверного программного обеспечения
- Поддержка SSL (через libnet-ssleay-perl)
- Поддержка прокси (с аутентификацией)
- Поддержка файлов cookie