



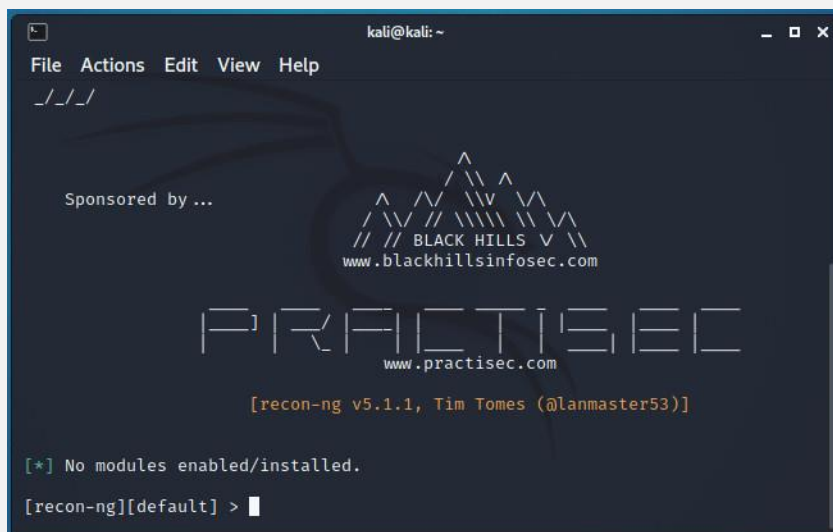
**АКАДЕМИЯ**  
**КОДЕБАЙ**

ПРОФЕССИЯ ПЕНТЕСТЕР

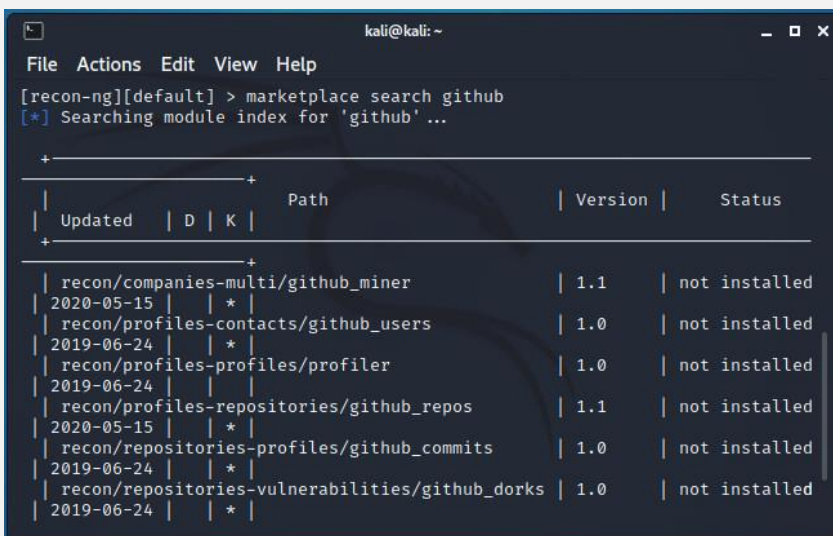
Следующий инструмент [Recon-ng](#) — это фреймворк для сбора информации через Интернет. Recon-ng отображает результаты работы в терминале, но также хранит их в базе данных. Большая часть возможностей Recon-ng заключается в передаче результатов одного модуля в другой, что позволяет нам быстро расширить объем собираемой информации.

Давайте воспользуемся Recon-ng для сбора интересных данных о MegaCorp One. Чтобы начать, давайте просто запустим recon-ng:

```
kali@kali:~$ recon-ng
```



Для использования Recon-ng нам необходимо установить различные модули. Мы можем добавить модули из "Marketplace" Recon-ng. Мы будем искать с помощью команды `marketplace search github`. В этом примере мы будем искать модули, содержащие термин `github`:

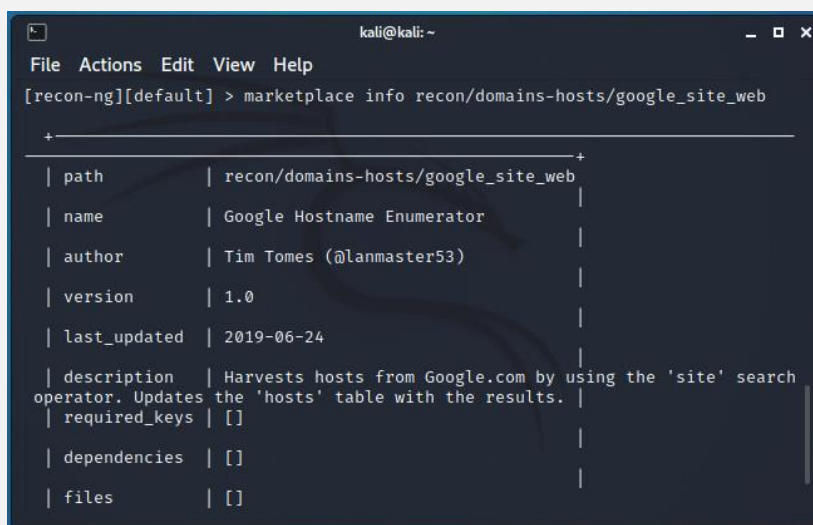


Updated	D	K	Path	Version	Status
2020-05-15		*	recon/companies-multi/github_miner	1.1	not installed
2019-06-24		*	recon/profiles-contacts/github_users	1.0	not installed
2019-06-24			recon/profiles-profiles/profiler	1.0	not installed
2020-05-15		*	recon/profiles-repositories/github_repos	1.1	not installed
2019-06-24		*	recon/repositories-profiles/github_commits	1.0	not installed
2019-06-24		*	recon/repositories-vulnerabilities/github_dorks	1.0	not installed

Обратите внимание, что некоторые модули отмечены звездочкой в колонке "K". Эти модули требуют учетные данные или API-ключи. На [вики-сайте Recon-ng](#) содержится краткая информация об этом.

Мы можем узнать больше о модуле, используя команду `marketplace info`, за которой следует название модуля. Поскольку модули GitHub требуют API-ключей, давайте воспользуемся этой командой для изучения модуля `recon/domains-hosts/google_site_web`:

```
[recon-ng][default] > marketplace info recon/domains-hosts/google_site_web
```



```
kali@kali: ~  
File Actions Edit View Help  
[recon-ng][default] > marketplace info recon/domains-hosts/google_site_web  
+-----+  
| path          | recon/domains-hosts/google_site_web |  
| name          | Google Hostname Enumerator          |  
| author        | Tim Tomes (@lanmaster53)            |  
| version       | 1.0                                  |  
| last_updated  | 2019-06-24                          |  
| description   | Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results. |  
| required_keys | []                                    |  
| dependencies  | []                                    |  
| files         | []                                    |
```

Согласно описанию, этот модуль осуществляет поиск в Google с помощью оператора "site" и не требует ключа API. Давайте установим модуль с помощью `marketplace install`:

```
[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
```

После установки модуля мы можем загрузить его с помощью команды `module load`, за которой следует его имя. Затем мы используем `info` для отображения подробной информации о модуле:

```
[recon-ng][default] > modules load recon/domains-hosts/google_site_web  
[recon-ng][default][google_site_web] > info
```

Согласно выводу, модуль требует использования источника, который является целью о которой мы хотим собрать информацию. В данном случае мы будем использовать `options set SOURCE megacorpone.com`, чтобы задать целевой домен:

```
[recon-ng] [default] [google_site_web] > options set SOURCE megacorpone.com
```

И наконец давайте запустим модуль:

```
[recon-ng][default][google_site_web] > run  
MEGACORPONE.COM  
[*] Searching Google for: site:megacorpone.com  
[*] [host] megacorpone.com (<blank>)  
[*] [host] vpn.megacorpone.com (<blank>)  
[*] [host] www2.megacorpone.com (<blank>)
```

Результаты совпадают с тем, что мы нашли в предыдущем уроке при поиске DNS в Netcraft. Однако мы не зря потратили время. Recon-ng сохраняет результаты в локальной базе данных, и эти результаты будут использоваться в других модулях Recon-ng.

Давайте теперь установим все модули из "Marketplace" Recon-ng. Сделать это можно с помощью команды marketplace install all:

```
MEGACORPONE.COM  
[*] Country: None  
[*] Host: fs1.megacorpone.com  
[*] Ip_Address: 51.222.169.210  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] -----  
[*] Country: None  
[*] Host: ns1.megacorpone.com  
[*] Ip_Address: 51.79.37.18  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] -----  
[*] Country: None  
[*] Host: mail2.megacorpone.com  
[*] Ip_Address: 51.222.169.213  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] -----  
[*] Country: None  
[*] Host: ns2.megacorpone.com  
[*] Ip_Address: 51.222.39.63  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] -----  
[*] Country: None  
[*] Host: www2.megacorpone.com  
[*] Ip_Address: 149.56.244.87  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] -----
```

```
[recon-ng][default] > marketplace install all
```

Теперь давайте попробуем получить тот же результат, но с помощью другого модуля:

```
[recon-ng][default] > modules load  
recon/domains-hosts/hackertarget
```

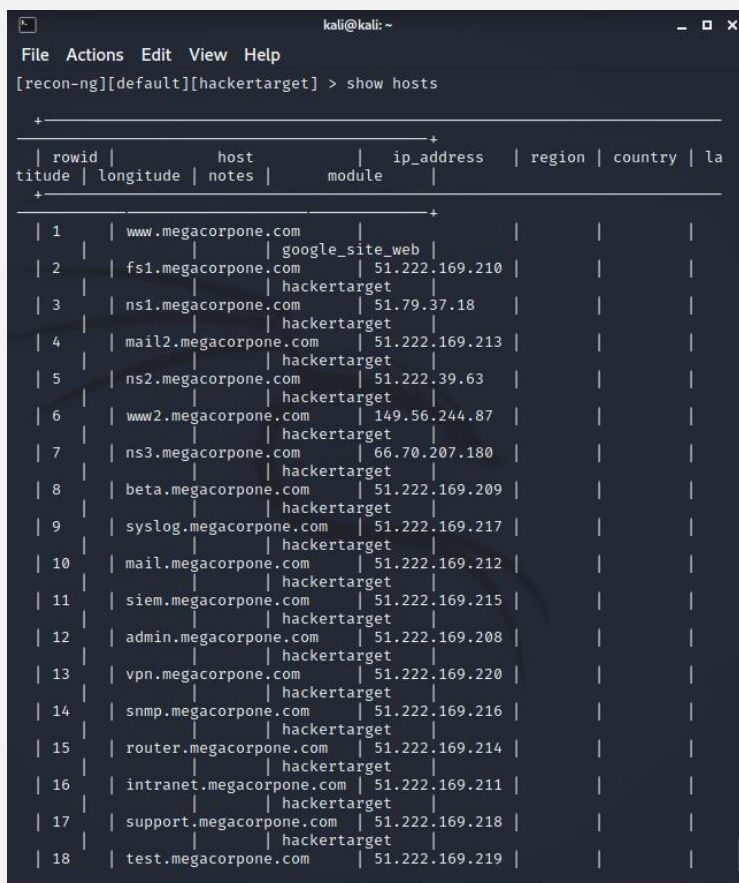
```
[recon-ng][default][hackertarget] > options set  
SOURCE megacorpone.com
```

```
[recon-ng][default][hackertarget] > run
```

Как видите с помощью этого модуля мы получили еще и IP-адреса, что в целом позволяет нам не использовать модуль recon/hosts-hosts/resolve.

Далее давайте используем команду `show hosts` для просмотра сохраненных данных:

```
[recon-ng][default][hackertarget] > show hosts
```



rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	www.megacorpone.com							google_site_web
2	fs1.megacorpone.com	51.222.169.210						hackertarget
3	ns1.megacorpone.com	51.79.37.18						hackertarget
4	mail2.megacorpone.com	51.222.169.213						hackertarget
5	ns2.megacorpone.com	51.222.39.63						hackertarget
6	www2.megacorpone.com	149.56.244.87						hackertarget
7	ns3.megacorpone.com	66.70.207.180						hackertarget
8	beta.megacorpone.com	51.222.169.209						hackertarget
9	syslog.megacorpone.com	51.222.169.217						hackertarget
10	mail.megacorpone.com	51.222.169.212						hackertarget
11	siem.megacorpone.com	51.222.169.215						hackertarget
12	admin.megacorpone.com	51.222.169.208						hackertarget
13	vpn.megacorpone.com	51.222.169.220						hackertarget
14	snmp.megacorpone.com	51.222.169.216						hackertarget
15	router.megacorpone.com	51.222.169.214						hackertarget
16	intranet.megacorpone.com	51.222.169.211						hackertarget
17	support.megacorpone.com	51.222.169.218						hackertarget
18	test.megacorpone.com	51.222.169.219						hackertarget